Aurorean™ Virtual Network

RiverMaster Administrator’s Guide

Version 3.1

ENTERASYS NETWORKS™

Part Number: AVN-RMAG-R31

Released: March 2001

Printed in the USA.

For more information on Enterasys Networks products, refer to the following table:

U.S. Office	
Address	35 Industrial Way Rochester, NH 03866
Phone	1-877-641-7400
Fax	(603) 337-2211
Internet	http://www.enterasys.com
Sales	1-877-641-7400 www.enterasys.com
Support	Call the Enterasys GTAC at 1-800-872-8440 or email us at support@enterasys.com

Aurorean Virtual Network software includes the following third-party components:

Table of Contents

About This Guide

Chapter 1 – Installing RiverMaster Software

Chapter 2 – Getting Started with RiverMaster

Chapter 3 – Configuring an ANG-3000/7000

Chapter 4 – Setting Up Aurorean Services

Chapter 5 – Controlling Remote User Dialing & Access

Chapter 6 – Managing Users & Groups

Chapter 7 – Viewing Server Activity & Statistics

Chapter 8 – Generating Reports

Appendix A – Glossary

Appendix B – ANG-3000/7000 Preconfiguration Stored on a Floppy Disk

Chapter 9 – License Agreement & Support

Index

About This Guide

This guide describes how to use Version 3.1 of the RiverMaster management application to set up and monitor Aurorean Virtual Network systems. While written primarily to describe how to configure a Aurorean Virtual Network solution for the first time, this guide also addresses how to track usage and troubleshoot end-to-end VPN connectivity problems.

The guide is designed for network administrators who are responsible for installing and managing local and wide area networking equipment. The guide assumes you have experience working with LAN devices such as firewalls, routers, hubs, and file servers.

Contents of the Guide

Information in this guide is arranged as follows:

❒ *Chapter 1, Installing RiverMaster Software* provides step-by-step instructions for installing the RiverMaster application on your computer and starting the application for the first time.

❒ *Chapter 2, The Guided Tour* contains an overview of RiverMaster operation, describes how to log into RiverMaster and check the status of your Aurorean Virtual Network servers, and walks you through the process of setting up an Aurorean Virtual Network for the first time.

❒ *Chapter 3, Configuring a Aurorean Network Gateway*describes how to configure network settings, such as IP addresses, name resolution servers, tunnel protocols, and routing protocols, using RiverMaster or Aurorean Policy Manager. The chapter describes how to back up the database on the Aurorean Policy Server and details how to set up site-to-site tunnels from one Aurorean Network Gateway to another. It also details how to view and change alternate ANG address data.

❒ *Chapter 4, Setting Up Aurorean VN Services* discusses how to: use the Authorization service to authenticate remote users, prepare the Notification service to send E-mail in response to Aurorean Virtual Network alarm, alert, or notification messages, and set trace levels for system messages.

- ❒ *Chapter 5, Controlling Remote User Dialing & Access* describes how to define Aurorean Network Gateway destinations, select ISPs from the TollSaver database, configure POP packages and add corporate dial-up phone numbers.
- ❒ *Chapter 6, Managing Users & Groups* addresses how to create a user database on a Aurorean Policy Server, assign policies that govern user access to the network, and prepare a customized Aurorean Client Software installation kit.
- ❒ *Chapter 7, Viewing Server Activity & Statistics* shows you how to examine and interpret message traffic between Aurorean Virtual Network devices and monitor the performance of active tunnel connections. Standard SNMP MIB-II and two private MIBs are now available to monitor your Aurorean systems.
- ❒ *Chapter 8, Generating Reports* describes how to download and view customized reports that reveal Aurorean Virtual Network server performance and remote user activity.
- ❒ *Appendix A, Glossary* contains definitions for terms used throughout this guide.
- ❒ *Appendix B, Configuring the ANG with a Floppy Disk,* describes a procedure similar to the steps you would take to configure the ANG by using the RiverMaster application. But this method allows an administrator to centrally set up one or more gateways and distribute that information on floppy disks to remote sites.
- ❒ *Appendix C, License Agreement & Support* describes the agreement that governs the use and distribution of RiverMaster software and provides information for contacting Enterasys Networks for technical support.

Conventions Used in this Guide

The following conventions are used in this guide:

☑ **NOTE** — Notes supply additional helpful information, point you to where you can find more information, or emphasize critical issues you should consider when performing an action.

⚠ **CAUTION** — Cautions contain directions that can prevent you from damaging the product or losing data.

⚠ **WARNING** — Warnings provide directions that you must follow to avoid harming yourself.

Bold — Text in boldface indicates values you type using the keyboard (for example, **a:\setup**). Default settings may also appear in bold.

Italics — Text in italics indicates a variable, important new term, or the title of a manual.

SMALL CAPS — Text in small caps specifies keys to press on the keyboard; a plus sign (+) between keys indicates that you must press the keys simultaneously (for example, CTRL+ALT+DEL).

`Courier font` — Text in this font denotes a file name or directory.

Related Documents

The following publications are also supplied with Aurorean VN systems:

- *RiverMaster Quick Reference Card* that contains shortcuts and tips for installing and using the RiverMaster application.
- *Quick Setup* cards that highlight the basic steps required to install either a Aurorean Policy Server or Aurorean Network Gateway.
- *Aurorean Installation & Service Guide* describes how to mount, connect, power-up, and maintain an Aurorean Policy Server and Aurorean Network Gateway.
- *ANG-1000 User's Guide* details how to install and configure the small office / home office Network Gateway.

Portable Document File (PDF) versions of these manuals are available on the Aurorean System Software CD ROM. Using Adobe Acrobat Reader 3.0 (or later), you can view these manuals on-line or print additional copies. Acrobat Reader can be downloaded from the Adobe web site (www.adobe.com).

1

Installing RiverMaster Software

This chapter provides the system requirements and step-by-step instructions for installing RiverMaster software on your computer. If you have not already done so, Enterasys Networks recommends that you mount and connect your Aurorean Policy Server and Aurorean Network Gateway before performing these steps. Refer to the *Aurorean Installation & Service Guide* supplied with each server for detailed installation instructions.

System Requirements

To run the RiverMaster application, your computer must meet the following requirements.

Hardware Requirements

RiverMaster runs on a desktop or laptop computer equipped with:

- ❒ A 233 MHz processor or faster
- ❒ 64 MB RAM minimum, 128 MB recommended
- ❒ 80 MB free space on the computer’s hard drive
- ❒ CD ROM drive
- ❒ Ethernet network interface

NOTE

To best view the RiverMaster user interface, set your monitor to display 65536 colors or better at 1024 x 768 resolution.

Software Requirements

The following operating systems, applications, and protocols should be installed and configured before you install RiverMaster:

- Windows NT 4.0 Workstation upgraded with Service Pack 4 (SP4) or later version or Windows 2000 Professional
- TCP/IP protocol
- To use Aurorean Policy Manager: Internet Explorer 5 or Netscape 4

Installing the Application

Before installing RiverMaster, close any applications you have running. Once the installation is complete, you must restart the computer before you can use RiverMaster to manage your Aurorean Virtual Network.

NOTE

You must log into your Windows NT Workstation/2000 computer using an account with administrator privileges before installing RiverMaster. Without administrator privileges, some files may not install properly and you may be prevented from using some RiverMaster features.

Upgrading a Previous Release

The following instructions assume you are installing RiverMaster on your computer for the first time. Do not re-install RiverMaster over a previous version. Remove the older version of RiverMaster as described in “Removing RiverMaster Files” on page 9 and then install the new version as described in the following section.

Installation Steps

To install RiverMaster on your computer, perform the following steps:

1. Insert the Aurorean 3.0 System Software CD into the CD ROM drive.
2. Open Windows Explorer, go to the RiverMaster directory on this CD and run the `SETUP.EXE` program.

3 If a warning message appears stating that Microsoft ODBC is not present on your computer, click OK to install Microsoft ODBC. If this message does not appear, continue with the next step.

The Microsoft ODBC text driver must be installed on your computer in order for RiverMaster to generate reports. RiverMaster Setup automatically launches the Microsoft ODBC install program; follow the instructions provided on the screen. When asked, choose the Typical ODBC installation. After ODBC is installed, RiverMaster Setup automatically resumes.

4 When the Welcome window appears, click Next to continue.

To halt the installation and exit the Setup program, click Cancel; this option is also available on all Setup windows that follow.

5 When the Software License Agreement window appears, carefully read the agreement and click Yes to accept the terms.

To install RiverMaster, you must accept the agreement. If you click No to decline the agreement, the Setup program will close.

6 On the Choose Destination Location window, select where you want RiverMaster files stored on the computer's hard disk and click Next.

As a default, RiverMaster files are stored in `C:\Program Files\Indus River Networks\RiverMaster`. To change the destination folder, click Browse to select an existing folder or create a new folder. To return to the previous window to change your selections, click Back; this option is also available on all Setup windows that follow.

7 When the Select Program Folder window appears, assign a name to the RiverMaster program folder and click Next.

As a default, the Setup program creates an Indus River Networks folder that appears in the Programs menu. This folder contains shortcut icons for the RiverMaster application and a README file.

8 When the Start Copying Files window appears, click Next to continue the installation or click Back to change your selections.

9 An Information window appears stating that to read the RiverMaster documentation, you must install the Adobe Acrobat Reader program. Click OK.

Acrobat Reader can be found in the 3rd Party Support Software directory on this CD or at the Adobe Website (www.adobe.com).

10 When the Setup Complete window appears, do one of the following:

- To view the README file immediately, leave the check box checked and click Finish.
- To wait until later to view the README file, remove the check from the check box and click Finish.

11 At the second Setup Complete window, choose Yes to restart your computer and click Finish.

When the reboot completes, RiverMaster is installed and ready to manage your Aurorean Virtual Network.

✓ NOTE

If RiverMaster is running while you upgrade your Aurorean Policy Server software, RiverMaster may become confused. To avoid this situation, exit RiverMaster at the beginning the APS installation or exit and restart RiverMaster after the process has completed.

Starting the Application for the First Time

When you start the RiverMaster application for the first time, you are asked for the following information:

❐ The IP address(es) you assigned to the Aurorean Policy Server(s) during its installation.

❐ The Aurorean VPN you assigned to your servers when they were installed.

❐ A user name and password to log into RiverMaster (the defaults are user **netadmin** and password **netadmin**).

✓ NOTE

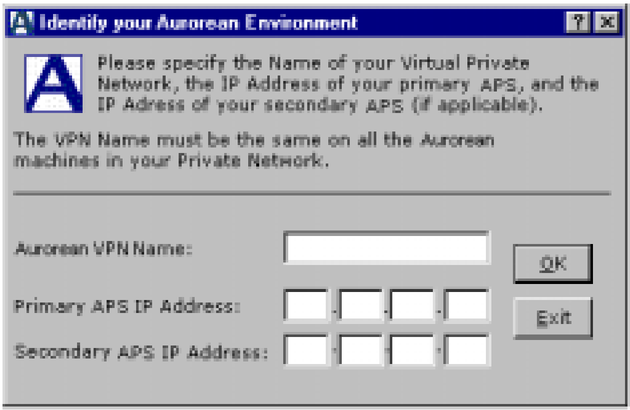
RiverMaster lets you invoke two RiverMaster sessions from one Windows NT/2000 computer to a primary and secondary Aurorean system. This feature is especially useful when running AutoLink Recovery™ (ALR), which employs automatic fail over to a backup Aurorean Virtual Network system. If you wish to invoke two RiverMaster sessions, you will be required to enter two IP addresses.

To start RiverMaster, perform the following steps:

RiverMaster

1 On the main Windows NT/2000 desktop, double-click the RiverMaster icon.

Alternatively, you can click the Start button, point to Programs, point to Indus River Networks, and then click RiverMaster. In the RiverMaster program group, click RiverMaster to launch the application. After a few seconds, the Identify Your Aurorean Environment window appears as shown in Figure 1.



Identify your Aurorean Environment

Please specify the Name of your Virtual Private Network, the IP Address of your primary APS, and the IP Adress of your secondary APS (if applicable).

The VPN Name must be the same on all the Aurorean machines in your Private Network.

Aurorean VPN Name:

Primary APS IP Address: . . .

Secondary APS IP Address: . . .

Figure 1 First-Time Setup Information

2 In the Aurorean VPN Name field, type a collective name that will be shared by all Aurorean devices on your corporate network.

This name is set using the APS Quick Configuration wizard program; refer to the *Aurorean Installation & Service Guide* for more information.

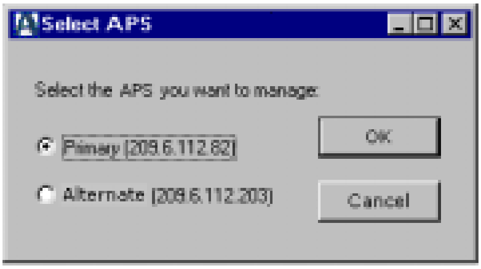
3 Do one of the following:

- If you are configuring only one Aurorean Policy Server, enter the IP address assigned to it in the Primary fields and click OK. The RiverMaster Login window will appear as shown in Figure 3 with the Aurorean VN Name, APS name and IP address displayed as you specified earlier. Skip to Step 5.
- If, in addition to configuring a Primary APS, you have installed a backup APS to use with the Auto Link Recovery feature, supply this IP address in the Alternate fields after entering an IP address of the Primary APS in the fields provided. Click OK. The Select APS window will appear as shown in Figure 2.

This IP address is set using the Aurorean configuration wizard program; refer to the instructions supplied with this program for more information. RiverMaster needs this IP address to locate and synchronize with the Aurorean Policy Server.

4 If you entered both APS IP addresses, select the APS you want to log into and click OK.

The RiverMaster Login window appears as shown in Figure 3 with the Aurorean VPN name displayed as typed in the Identify your Aurorean Environment window.



Select the APS you want to manage:

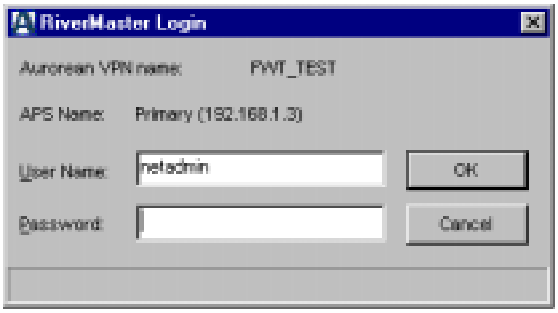
● Primary [209.6.112.82]

○ Alternate [209.6.112.203]

Figure 2 Select APS Window

5 Type the default user name (**netadmin**) and password (**netadmin**) and click OK.

For example, the primary APS name and its IP address is displayed in the RiverMaster Login window in Figure 3. When the RiverMaster application starts, the main interface appears as shown in Figure 4.



Aurorean VPN name: PWT_TEST

APS Name: Primary (192.168.1.3)

User Name: netadmin

Password:

Figure 3 RiverMaster Login Window

NOTE

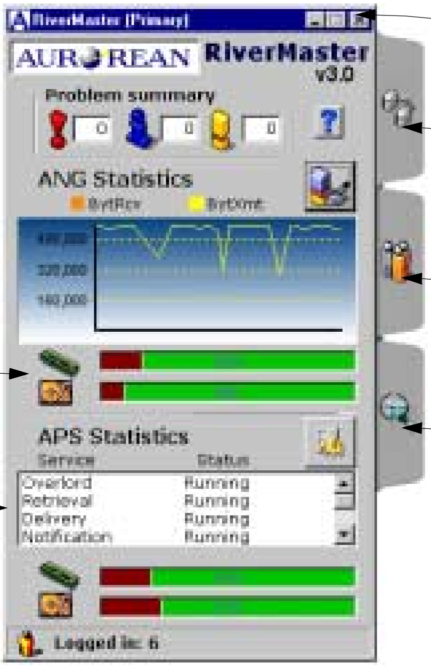
To prevent unauthorized RiverMaster access, Enterasys Networks recommends that you immediately create a new administrator account in the Admin group and delete the default login account. Refer to Chapter 6 for instructions on adding and deleting user accounts.

When you start RiverMaster, the application immediately attempts to detect and communicate with the Aurorean Policy Server and Aurorean Network Gateway located within the same corporate network. Depending upon the amount of remote client activity occurring on the VPN, RiverMaster may need up to a minute to detect and synchronize with both servers.

CAUTION

If you want to configure a connection to a second APS after having already configured a connection to only one server, you must first delete the `config.irx` file in the `C:\Program Files\Indus River Networks\RiverMaster` directory on the RiverMaster PC. Then, when you click on the RiverMaster desktop icon, the Identify your Aurorean VN Environment window will appear as described on page 5.

Using the Delivery service running on all Aurorean components, RiverMaster establishes a Delivery session with each server. The Aurorean Policy Server reports service status, memory / hard disk usage, and a summary of alarms, alerts, and problem notification messages. The Aurorean Network Gateway reports an aggregated total of bytes sent and received over all tunnels, as well as memory / hard disk usage.



Service	Status
Overlord	Running
Retrieval	Running
Delivery	Running
Notification	Running

Click here to close the application

Configuration pullout

Manage Users & Groups pullout

View System Activity pullout

When memory and disk usage appears, RiverMaster has detected and synchronized with the Aurorean Network Gateway

When service status appears, RiverMaster has detected and synchronized with the Aurorean Policy Server

Figure 4 RiverMaster Main Interface

To learn more about the server status data displayed on the RiverMaster interface, refer to Chapter 2. To exit the RiverMaster application at any time, click the close (**X**) button in the upper-right corner of the main interface.

NOTE

If you have used RiverMaster extensively to generate reports and view messages during a period of peak activity, the application may require a few moments to close.

Removing RiverMaster Files

RiverMaster can be uninstalled from your computer using the standard Add / Remove Programs tool provided with Windows. After RiverMaster files are removed from your computer, you should restart the computer to clean up any files that were in use during the uninstall.

To remove RiverMaster files from your computer, perform the following steps:

1 On your desktop computer, click the Start button, point to Settings, then click Control Panel.

2 Double-click on Add/Remove Programs to launch the utility.

3 On the Install/Uninstall tab page, select RiverMaster from the list of programs and click Add/Remove.

4 When the Confirm File Deletion window appears, click Yes to confirm that you want to remove RiverMaster.

Clicking Yes launches the UnInstallShield program, which manages the process of deleting RiverMaster files.

5 When Remove Shared File? windows appear for shared .DLL and .OCX files, click Yes To All and click Yes again to confirm your decision.

6 When the Remove Programs From Your Computer window appears with all items checked, click OK.

7 When a window appears indicating that RiverMaster has been removed, click OK to acknowledge the message but do not restart your computer.

Although the Add / Remove Programs utility removes most Aurorean VN files, you must manually delete the contents of the RiverMaster folder within the Indus River Networks folder on your hard drive. You should do this before restarting your computer.

8 Close the Add/Remove Programs control panel.

9 Open Windows Explorer by clicking the Start button, pointing to Programs, and then clicking Windows Explorer.

10 Locate the RiverMaster program folder.

The default location for this folder is `C:\Program Files\Indus River Networks`.

11 Delete the RiverMaster folder.

12 Restart your computer.

2

Getting Started with RiverMaster

This chapter introduces the essential functions of RiverMaster, describes Aurorean Virtual Network system status information displayed on the main interface, and summarizes the steps required to use RiverMaster to configure your Aurorean Virtual Network for the first time.

RiverMaster Overview

When RiverMaster is installed on your PC, the computer becomes a “management station” for the Aurorean Virtual Network, receiving dynamic updates from Aurorean Virtual Network systems and making immediate configuration changes. All data displayed by RiverMaster is retrieved from databases residing on the Aurorean Policy Server or from incoming messages from either the Aurorean Policy Server or Aurorean Network Gateway; no data is stored locally on your PC’s hard disk.

Figure 5 illustrates the interaction between the Aurorean Policy Server, Aurorean Network Gateway, and RiverMaster PC.

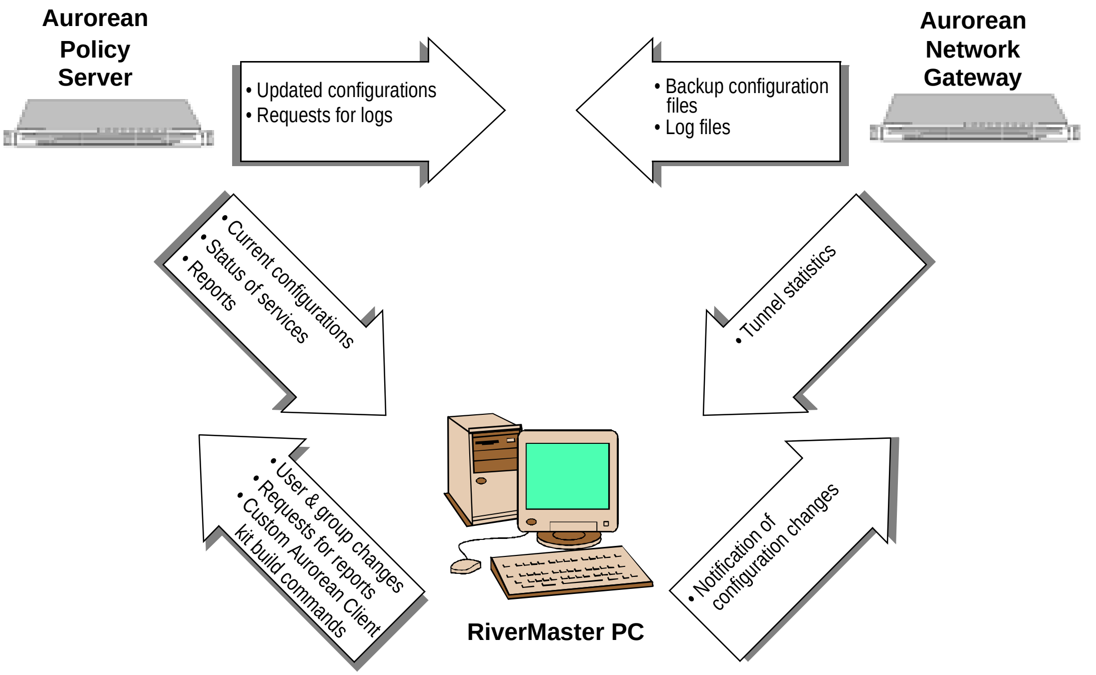


Figure 5 Aurorean Virtual Network Communication Flow

Using the RiverMaster management application you can:

- ❒ Quickly check a server’s operational status by determining if all services are running, reviewing alarm and alert messages that have accumulated, and displaying current tunnel activity (the number of users logged in and the amount of data passing over all tunnels).
- ❒ Define “virtual subnets” to provide IP addresses to remote Aurorean Client Software users and allow the Aurorean Network Gateway to properly route remote user packets through the corporate network.
- ❒ Select which Internet Service Providers (ISPs) your remote Aurorean Client Software users can use from the extensive TollSaver database stored on the Aurorean Policy Server.
- ❒ Define user accounts on the Aurorean Policy Server to locally authenticate remote users or install a “plug-in” to authenticate users against an external RADIUS or SecureID server.

❒ Organize users with groups and assign each group policies that govern the features available in Aurorean Client Software.

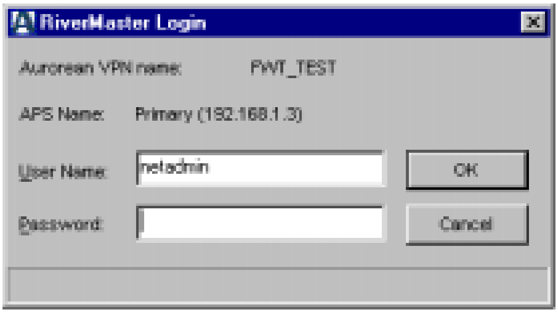
❒ Create customized Aurorean Client Software installation kits to distribute to your remote users that contains the Aurorean Client Software application, POP packages, group policies, and destination IP addresses.

Logging into RiverMaster

When you start the RiverMaster application, the RiverMaster Login window appears as shown in Figure 6 if you have configured a connection to *one* Aurorean Policy Server. If you have configured a connection to a *second* Aurorean Policy Server, the Select APS window will appear as shown in Figure 7.

Version 3.0 of RiverMaster lets you start two RiverMaster sessions from one Windows NT/2000 computer to separate Aurorean Virtual Network systems. This feature is especially useful when running AutoLink Recovery, which employs automatic fail over to a backup Aurorean Virtual Network system.

To access RiverMaster, you must enter a user name and password that the Aurorean Policy Server can authorize from its internal database. The default login account is **netadmin** with the password **netadmin**.



RiverMaster Login

Aurorean VPN name: PWT_TEST

APS Name: Primary (192.168.1.3)

User Name: netadmin

Password:

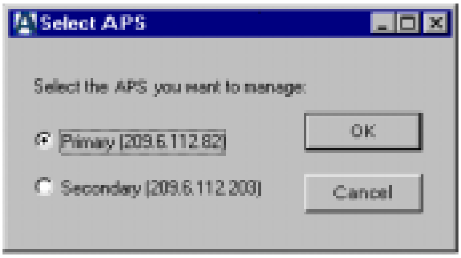
Figure 6 RiverMaster Login Window

Log into RiverMaster by typing a user name and password in the fields provided, and choosing the Aurorean VPN name associated with the Primary Aurorean Policy Server. Click OK.

NOTE

To prevent unauthorized RiverMaster access, Enterasys Networks recommends that you immediately create a new administrator login account in the IRAdmin group and delete the default login account. Refer to Chapter 6 for more on adding and deleting user accounts.

If you have configured a connection to a second Aurorean Policy Server, the Select APS window appears as shown in Figure 7. Select the Aurorean Policy Server you want to manage and click OK. The RiverMaster Login window then appears as shown in Figure 6 allowing you to log into the selected Aurorean Policy Server.


Select APS

Select the APS you want to manage:

● Primary [209.6.112.82]

○ Secondary [209.6.112.203]

Figure 7 Select APS Window

CAUTION

If you want to configure a connection to a second Aurorean Policy Server after having already configured a connection to only one server, you must first delete the `config.irx` file in the `C:\Program Files\Indus River Networks\RiverMaster` directory on the RiverMaster computer. Then, when you click on the RiverMaster desktop icon, the Identify your Aurorean Environment window will appear as described in Chapter 1.

Checking Server Status

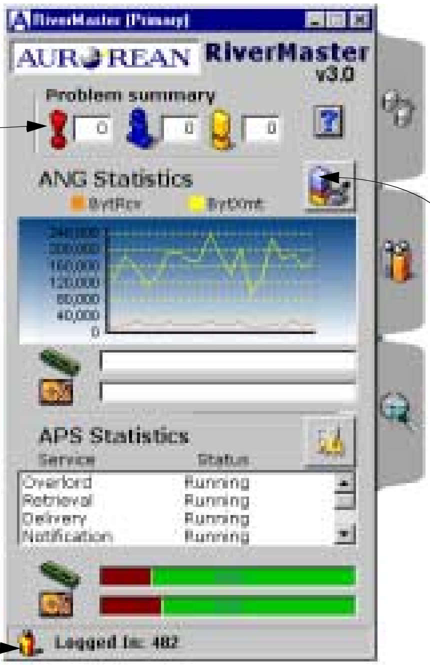
RiverMaster's main interface is designed to quickly show the Aurorean Virtual Network's "health" when you start the application. The health conditions are organized into three categories:

- Problem summary and users logged in
- Aurorean Network Gateway statistics
- Aurorean Policy Server statistics

Problem Summary & Users Logged In

As shown in Figure 8, counters at the top and bottom of the interface track both error conditions and successful tunnel login attempts. The Problem Summary counters are updated whenever RiverMaster receives one of three types of messages:

- *Alarms* notify you when a significant error occurs with a service running on a Aurorean Virtual Network system or a general server problem that is preventing the server from operating normally.
- *Alerts* occur when an error count threshold has been crossed and an alarm condition is imminent.
- *Problem Notification messages* typically indicate an error at the Aurorean Network Gateway or a remote client connection problem which Aurorean Client Software's Prescriber feature diagnosed and reported. Prescriber is a Aurorean Virtual Network feature which diagnoses why a tunnel connection failed and attempts to correct the problem.



Service	Status
Overlord	Running
Retrieval	Running
Delivery	Running
Notification	Running

Indicates current alarms, alerts, and informational messages that appear in the System Activity window (refer to Chapter 7 for more information)

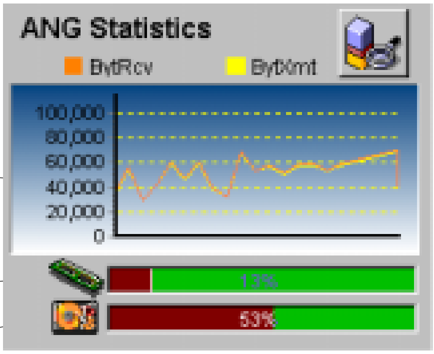
Click here to view more details about logged in users

Total number of remote users authenticated and connected to the corporate network via the Aurorean Network Gateway

Figure 8 Aurorean Network Gateway Status Information

Aurorean Network Gateway Statistics

Figure 9 shows the statistics information RiverMaster displays for the Aurorean Network Gateway. The graph indicates total amount of bytes sent and received over all tunnels processed by the Aurorean Network Gateway; to view the traffic passing over a single tunnel, click the button at the top right corner of the graph.



Aggregated number of bytes received and sent over all tunnels processed by the Aurorean Network Gateway

Click here to view detailed statistics for individual tunnels (refer to Chapter 7 for details)

Memory usage

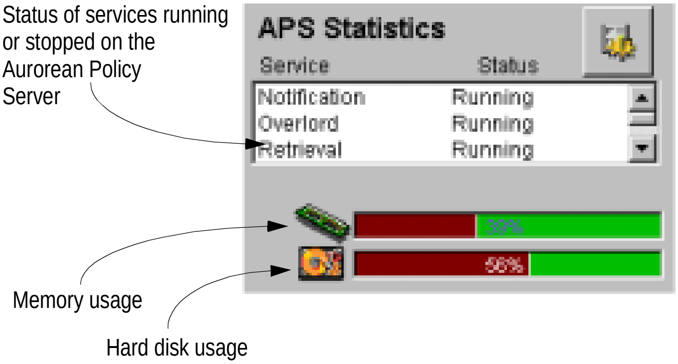
Hard disk usage

Figure 9 Aurorean Network Gateway Statistics

The memory and hard disk usage meters show how much system resources are being consumed supporting tunnel connections. You can use these values for capacity planning to determine when the number of concurrent tunnels is approaching the server’s limit.

Aurorean Policy Server Statistics

As shown in Figure 10, RiverMaster displays the current status of services running on the Aurorean Policy Server. Normally, all services should appear as “Running.” If one or more services appears as “Stopped,” then the Aurorean Policy Server may not function correctly. Table 1 briefly defines each service and describes what occurs when the service is stopped.



APS Statistics

Service	Status
Notification	Running
Overlord	Running
Retrieval	Running

Status of services running or stopped on the Aurorean Policy Server

Memory usage

Hard disk usage

Figure 10 Aurorean Network Gateway Statistics

Table 1 Aurorean Policy Server Services

Service	Function	If Stopped...
Overlord	Monitors the condition of all other Aurorean services and restarts a service if it fails to initialize properly or ceases to operate at any point. Overlord may also force a total server reboot if necessary.	The Aurorean Policy Server automatically reboots itself approximately 20 seconds after the Overlord service stops.
Retrieval	Retrieves statistics and messages from both the Aurorean Network Gateway and Policy Server to generate activity and anomaly reports.	You cannot download and view reports using RiverMaster.
Delivery	Carries messages between all Aurorean Virtual Network components, including servers, Aurorean Client Software clients, and the RiverMaster management application. Delivery is a critical service that must be operational for Aurorean Virtual Network components to initialize properly and synchronize with one another.	The Aurorean Policy Server cannot communicate with the RiverMaster application and remote users are unable to authenticate and establish a tunnel connection with the Aurorean Network Gateway. The Aurorean Policy Server automatically reboots itself approximately 3 minutes after the Delivery service stops.

Table 1 Aurorean Policy Server Services

Service	**Function**	**If Stopped...**
Notification	Reports alarm, alert, and problem notification messages using E-mail.	The Aurorean Policy Server and Network Gateway can operate normally but E-mail messages are no longer sent when alarms/alerts/problems occur.
FTP	Provides the mechanism for transferring files between Aurorean Virtual Network servers and RiverMaster. FTP also allows Aurorean Client Software computers to synchronize group policy settings, TollSaver POP phone numbers, Prescriber remedies, and Aurorean Client Software application executables.	Aurorean Client Software users can connect but cannot perform client synchronization. RiverMaster cannot download reports from the Aurorean Policy Server. RiverMaster cannot complete database transactions and queries.
Access	Supports the exchange of database information stored on the Aurorean Policy Server to other Aurorean Virtual Network components, such as TollSaver data, logs, and server configuration files.	The Aurorean Policy Server cannot accept any configuration changes from the RiverMaster application and remote users are unable to authenticate and establish a tunnel connection with the Aurorean Network Gateway. The Aurorean Policy Server automatically reboots approximately 3 minutes after this service stops.

Table 1 Aurorean Policy Server Services

Service	Function	If Stopped...
Log	Maintains a running record of system events and messages received by each Aurorean Virtual Network component. The RiverMaster application displays these logs and extracts information from them to produce daily reports.	The Aurorean Policy Server will accept configuration changes and the Aurorean Network Gateway will accept tunnel connection attempts. However, the messages generated by these actions are not stored in a log file on the Aurorean Policy Server and cannot be viewed as they occur from the RiverMaster. Reports will also be inaccurate.
Authentication	Provides the mechanism for authenticating remote users against user databases located on either the Aurorean Policy Server or an external authentication server (such as a RADIUS device). Authentication also serves another security role, by enforcing a strict ring level hierarchy for Delivery messages to prevent unauthorized access to sensitive information.	Configuration changes sent by the RiverMaster to the Aurorean Policy Server are rejected because the Aurorean Policy Server cannot authenticate them. Also, the Aurorean Network Gateway will not accept new tunnel connection attempts because the remote user cannot be authenticated. The Aurorean Policy Server reboots approximately 3 minutes after this service stops.

The memory and hard disk usage meters in the Aurorean Policy Server statistics area show how much server resources are being consumed to manage the Aurorean Virtual Network. High memory usage normally reflects a large number of authorization messages for both remote user authentication and server-to-server traffic; generating reports and Aurorean Client Software installation kits can also consume Aurorean Policy Server memory. High disk space usage is normally a result of many large log and report files accumulating on the hard disk.

NOTE

When 85% of the Aurorean Policy Server drive capacity is full, the server automatically begins deleting logs and reports older than 90 days. Log and report deletions are not configurable at this time.

Setting Up a Aurorean Virtual Network the First Time

When you start RiverMaster for the first time, you need to perform several basic configuration steps to put your Aurorean Virtual Network into operation. These basic steps are outlined below, with references to the detailed instructions provided throughout this manual.

1 Enter the Aurorean VPN name for your Aurorean Virtual Network equipment and enter the IP address(es) of the Aurorean Policy Server(s).

You are prompted to enter these values the first time you start the RiverMaster application.

2 After you login with the default user name and password, set the authentication, encryption, and compression options used during tunnel connections.

These options are set separately for each tunnel protocol (PPTP or IPSec) as described in Chapter 3.

3 Allocate IP addresses for remote users to use when they tunnel into the corporate network.

You can assign a specific address to each remote user or allow users to dynamically draw addresses from a pool. Address pools are created by defining virtual subnets as described in Chapter 3.

4 Configure the Aurorean Network Gateway to route packets from remote users through the corporate network.

The Aurorean Network Gateway supports RIP, OSPF, and static routes to forward packets to their destination; to configure these routing protocols, refer to the instructions in Chapter 3.

5 Determine how remote Aurorean Client Software users will be authenticated.

- To authenticate against a database residing on the Aurorean Policy Server, you must use the Authorization service as described in Chapter 4.
- To authenticate against an external RADIUS server, you must configure an authorization plug-in as described in Chapter 4.
- To authenticate against an external SecurID server, you must configure an authorization plug-in as described in Chapter 4.

6 Create mailing lists so that the Aurorean Policy Server sends you E-mail when alarm, alert, or notification messages are generated (optional).

E-mail messages are generated by the Notification service as described in Chapter 4.

7 Reboot the Aurorean Network Gateway to put the networking changes into effect.

8 Create POP packages of selected Internet Service Providers (ISPs) from the list of those available in the master TollSaver database as described in Chapter 5.

By limiting the ISPs available for use by remote users and grouping them in POP packages, you can minimize the size of the database of Point of Presence (POP) phone numbers distributed to your Aurorean Client Software users. In addition to POP phone numbers, you can add corporate direct dial phone numbers to this database.

9 Define groups for remote Aurorean Client Software users as described in Chapter 6.

For each group you can assign a range of IP addresses to allocate to Aurorean Client Software users when they connect (using the virtual subnets you defined in Step 3). You can also grant policies to each group that determine the Aurorean Client Software features and functions that can be used by members of that group.

10 Add user accounts to each group as described in Chapter 6.

If you plan to authenticate all remote users against an external RADIUS or SecurID server, you can skip this step. For each user account, you must enter a specific IP address or indicate that the Aurorean Network Gateway must allocate the user an address from the group's virtual subnet.

11 Generate a customized Aurorean Client Software installation kit for distribution to members of each group as described in Chapter 6.

This installation kit contains the Aurorean Client Software application, group policy settings, destinations, and a TollSaver database with POP phone numbers for the ISPs assigned to the group.

Once remote users begin tunneling into the corporate network using Aurorean Client Software software, you can view this activity using the Tunnel Statistics window described in Chapter 7. You can also produce detailed daily usage reports as described in Chapter 8.

Authentication requests and other user activity messages are also displayed in the System Activity window described in Chapter 7. This window also displays alarm and alert messages that warn you when server errors occur.

3

Configuring an ANG-3000/7000

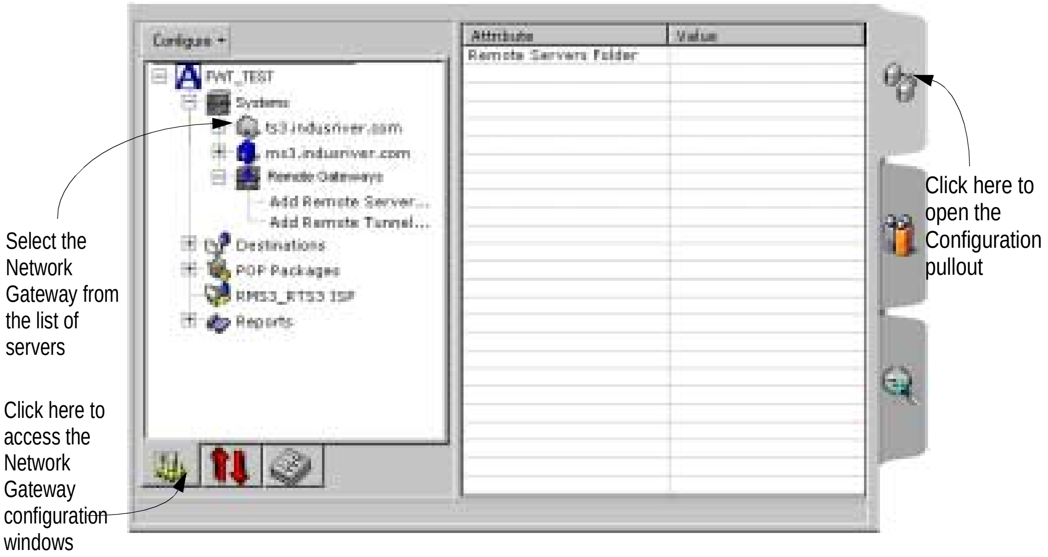
This chapter describes how to configure network settings for your *local* Aurorean Network Gateway (ANG-3000/7000). Local ANGs have an accompanying Aurorean Policy Server and are configured using RiverMaster. *Remote* ANGs are stand-alone systems configured by using the Web-based Aurorean Policy Manager utility. The ANG-1000 is configured using its Web-based configuration utility *only*. Network settings for the ANG fall into these categories:

- ❒ General settings such as the DNS, WINS and NAT servers that remote clients require for name resolution or authentication.
- ❒ Tunnel protocol (PPTP or IPSec) parameters for authentication, encryption, and compression.
- ❒ Virtual subnets containing pools of IP addresses or IPX network numbers that are allocated to remote users when they tunnel into the corporate network.
- ❒ Routing protocol (static, RIP, and OSPF) settings for each ANG Ethernet interface.
- ❒ Site-to-site tunnel parameters between two Aurorean Network Gateways.

NOTE

The ANG-3000/7000 can also be configured using a floppy disk. *Appendix B* describes a procedure similar to configuring the ANG using the RiverMaster application. Using the floppy disk method allows an administrator to centrally configure one or more gateways and conveniently distribute that configuration data on floppy disks to remote sites.

These functions are grouped on the Configuration pullout as shown in Figure 11.



Attribute	Value
Remote Servers Folder	

Select the Network Gateway from the list of servers

Click here to access the Network Gateway configuration windows

Click here to open the Configuration pullout

Figure 11 Configuration Pullout

Before You Begin

Before performing the steps in this chapter, you should familiarize yourself with the following Aurorean Virtual Network concepts:

- ❒ Methods available for allocating IP addresses and IPX network numbers to remote clients when they connect.
- ❒ Aurorean Virtual Network’s Intelligent Client Routing feature.
- ❒ Aurorean Virtual Network’s support for Network Address Translation (NAT).
- ❒ Methodology of Site-to-Site tunnels.
- ❒ Aurorean Virtual Network’s AutoLink Recovery feature.

Allocating IP/IPX Addresses to Remote Clients

When remote clients tunnel into the corporate network, they must be able to access devices on the network just as if they were locally connected. To serve this need, the ANG acts as a router, forwarding packets between devices on the corporate network and remote clients. When remote clients tunnel into the ANG, they must be allocated IP addresses accessible to or on the local network.

NOTE

To access Novell NetWare servers using IPX protocol, remote clients must receive an IPX network number. RiverMaster allows you to specify a single IPX network number that is shared by all remote clients when they connect. IPX usage is also controlled by a group policy; refer to Chapter 6 for more information on group policies.

You can allocate IP addresses to Aurorean users in one of three ways:

- ❐ Assign a specific IP address to each remote client. This address is saved as part of the client’s user name and password account information stored on the Aurorean Policy Server. Once the client authenticates, the address is allocated to the client for the duration of the connection. To receive an IP address in this manner, the remote client must authenticate against the Enterasys authorization plug-in as described in Chapter 4.
- ❐ Authenticate remote clients against an external authentication server (such as a RADIUS server) and have that server allocate IP addresses. To receive an IP address in this manner, the remote client must authenticate against a RADIUS plug-in as described in Chapter 4.
- ❐ Define one or more *virtual subnets* that act as address pools. Virtual subnets are linked to groups; when a member of a group connects, an address from within the virtual subnet is allocated to that user for the duration of the connection.

To support virtual subnets, the ANG must learn the topology of the corporate network and advertise to other devices that remote clients on the virtual subnet are reachable. To do this, the ANG supports Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) routing protocols. The ANG supports both RIP Version 1 and Version 2.

Virtual subnets can use both legitimate IP addresses (unique addresses purchased and registered by your company) and non-routable address ranges reserved for private network use only. These reserved address ranges include:

- 10.0.0.0 to 10.255.255.254 on a Class A network
- 172.16.0.0 to 172.30.255.254 on a Class B network. Although 172.31.0.0 to 172.31.255.254 is also a reserved range, you cannot define virtual subnets within this range because addresses in that range may be taken by the ANG for internal use.
- 192.168.0.0 to 192.168.255.254 on a Class C network

These addresses are not routable outside your corporate network. By using these addresses for remote clients, you can preserve the routable IP addresses for LAN devices.

NOTE

If you allocate addresses from one of these non-routable ranges and you want remote clients to be able to browse the Internet while connected, you must enable the Intelligent Client Routing described on page 31 or use network address translation.

There are several advantages to using virtual subnets over other IP address allocation techniques:

- The ANG can advertise the virtual subnets before remote clients connect. Using the other techniques, the ANG would only create a host route when the client connected. Because routing protocols may take as long as 30 seconds per router to propagate a host route, the client may remain unreachable for a period of time.
- Creating individual host routes for each remote client as they connect may overload the network's routers. Because ANG-5000s support 5000 tunnels (ANG-3000s support 500 tunnels), each router may become burdened with 5000 routes in its route table.Virtual subnets can be quickly and easily scaled up to accommodate large number of remote clients. You can modify the subnet mask for an existing virtual subnet to provide additional addresses or create entire new virtual subnets.

Figure 12 shows a sample corporate network that employs two virtual subnets. Each virtual subnet provides up to 255 client IP addresses depending upon the subnet mask used. By assigning different virtual subnets to each group, you can control what devices members of the group can access once they are connected.

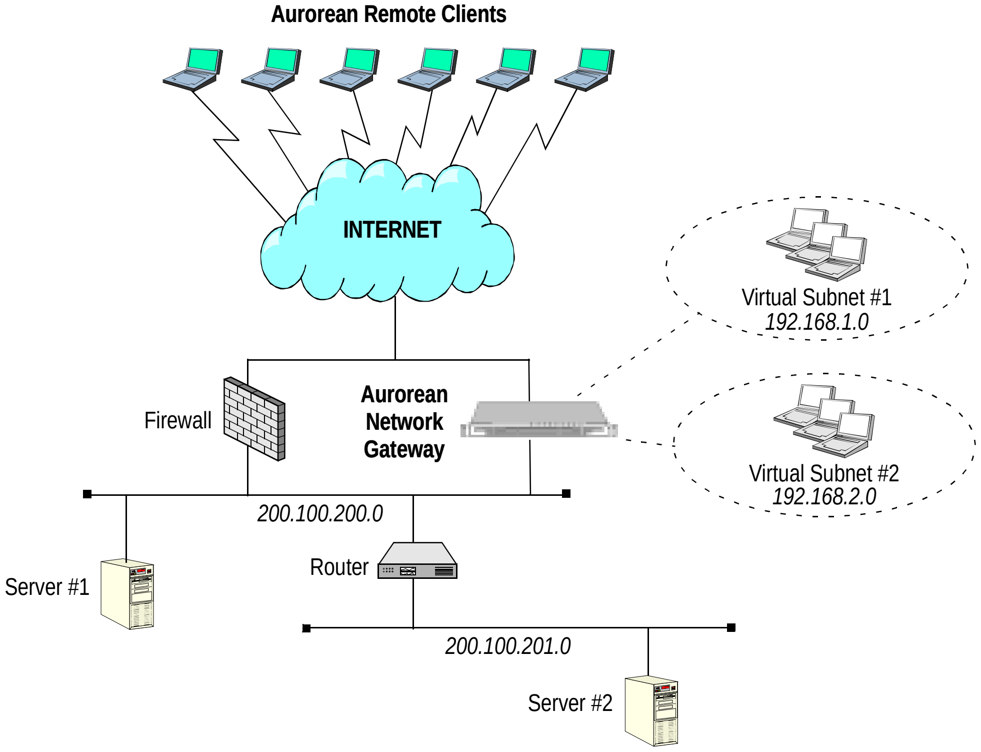


Figure 12 Remote Client Virtual Subnet Usage

For example, because Server #1 resides on the same network segment as the ANG, all remote clients can access this server regardless of the virtual subnet that provided their address. If you enable RIP or OSPF on the ANG Trusted interface, the router in this diagram will learn about both virtual subnets. However, if you enable only static routing on the ANG Trusted interface, you can limit access to the 200.100.201.0 subnet to users that receive address from Virtual Subnet #1. To accomplish this, you must create two static routes:

❒ Using RiverMaster, adding a static route for all addresses in the Virtual Subnet #1 range with the router's IP address as the default gateway.

❒ On the router, create a static route to forward all packets addressed with IP addresses in the Virtual Subnet #1 range to the IP address of the ANG Trusted interface.

With this arrangement, remote clients that receive addresses from Virtual Subnet #1 will be able to access Server #2. Without a static route, remote clients that receive addresses from Virtual Subnet #2 will be unable to access Server #2 or any other device on the 200.100.201.0 segment

Virtual Subnets for Site-to-Site and Remote Access Tunnel Servers

When you set up a site-to-site tunnel in conjunction with remote access service, we recommend creating separate groups and assigning separate virtual subnets for all your site-to-site and remote access users. This is necessary because RIP does not forward knowledge of a route over the interface from which it learned of that route. So if a remote client and a site-to-site tunnel obtain their virtual IP addresses from the same virtual subnet on the terminating ANG, then that remote access client will not be able to learn the routes that are known to the *initiator* of the site-to-site tunnel. This condition does not apply to a terminating ANG, though.

As shown in Figure 13, if ANG1 initiates a tunnel connection to ANG2, RIP will broadcast knowledge of ANG1's associated networks A, B and C to ANG2 just as it will propagate knowledge of ANG2's associated networks X, Y and Z to ANG1. Then, if the virtual subnet 10.10.10.0 is created on ANG2 for use by ANG1 site-to-site clients and is shared with remote Aurorean clients, the Aurorean users cannot access networks A,B, and C on ANG1 because they have no knowledge of those networks.

To remedy this situation, create virtual subnet 187.14.57.0 on ANG2 for Aurorean users. RIP will broadcast knowledge of this route to ANG2 enabling Aurorean users to dial into ANG1 as well as ANG2.

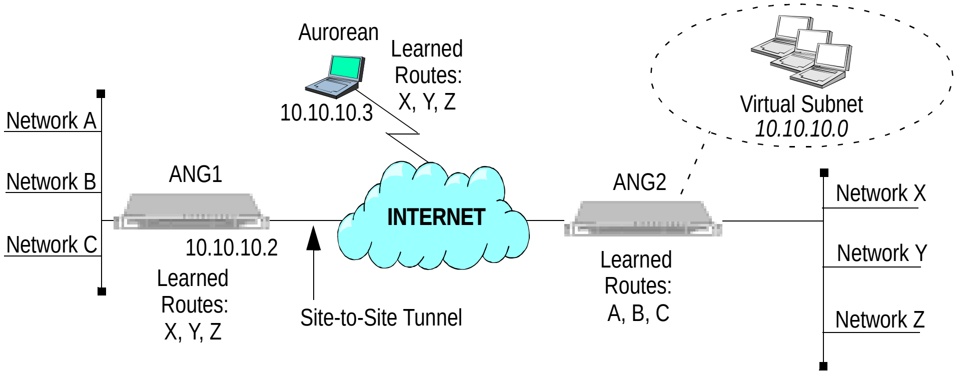


Figure 13 Virtual Subnets for Site-to-Site and Remote Access Tunnels

For instructions on creating virtual subnets for IP address and IPX network number allocation, refer to “Virtual Subnetting” on page 50.

Intelligent Client Routing

Enterasys Networks’ Intelligent Client Routing feature provides you with a measure of control over a Aurorean Client user’s access to the Internet. When enabled (this feature is enabled by default), Intelligent Client Routing allows remote clients to browse the Internet directly, outside of the tunnel. For example, if a remote client tries to browse the Internet while tunneled into the corporate network, packets bound for any destination within the Internet are sent down the tunnel into the ANG and then back out the network’s Internet gateway.

When Intelligent Client Routing is enabled, the ANG exports routes over the tunnel to the client. Based on this information, the client determines if the destination address can only be reached over the tunnel or can be reached directly on the Internet. Figure 14 contrasts how packets that are destined for an Internet server are routed with the Intelligent Client Routing feature enabled or disabled.

If you allocate a non-routable IP address to a remote client from a virtual subnet, you may need to enable Intelligent Client Routing to allow the remote client to browse the Internet.

Packets that are addressed with non-routable addresses are typically blocked by firewalls and Internet gateways and will be dropped by any Internet router. The only exceptions to this rule are devices such as “proxy” servers that perform a network address translation (NAT) to dynamically re-address packets as they leave the corporate network. If you do not have a NAT device, you can enable Intelligent Client Routing so that packets sent from the Aurorean Client computer to an Internet destination are addressed with the computer’s own IP address (not the non-routable address allocated from the virtual subnet).

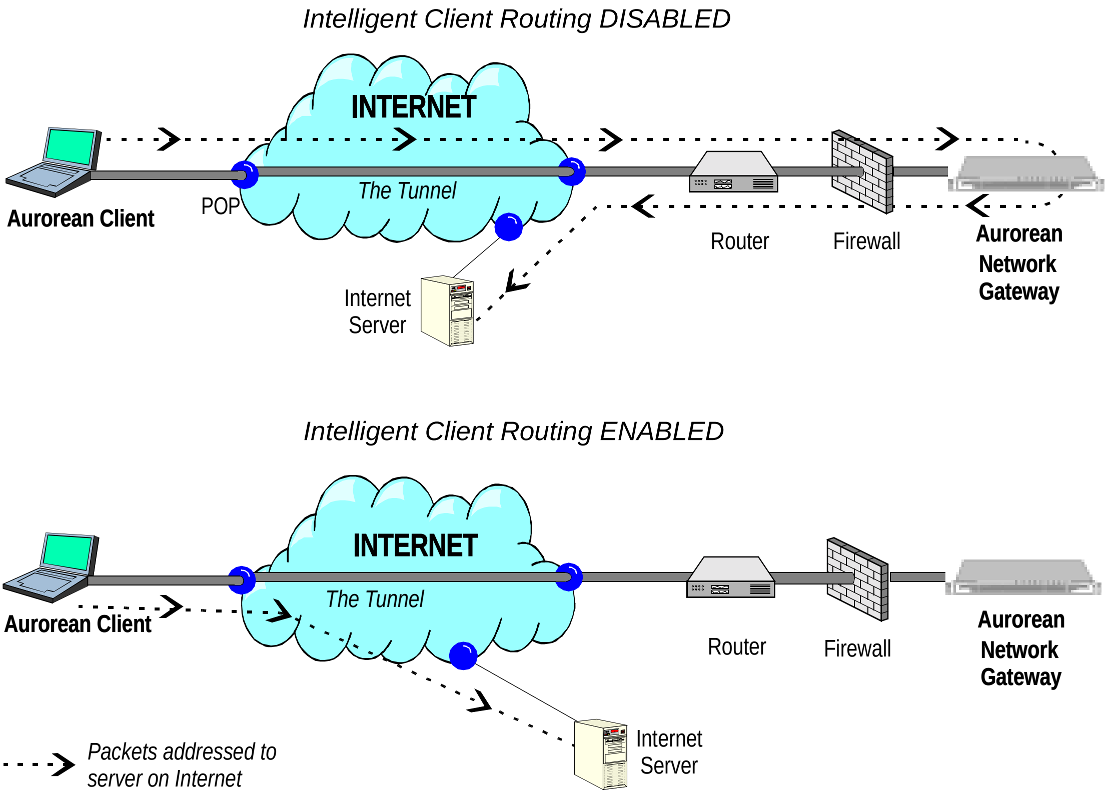


Figure 14 Aurorean Virtual Network’s Intelligent Client Routing Feature

NAT Server

RiverMaster's NAT server feature provides support for security conscious administrators who want to conceal the physical IP address of their system (ANG or another Gateway) without affecting Aurorean service. By configuring a NAT Server with an alias IP address for the ANG (refer to page 41 for instructions), the real IP address of the ANG will remain hidden and any IP address received by the NAT Server will be translated to the real IP address of the destination for all incoming clients. This ensures that clients access the correct IP address and build a tunnel connection to the ANG without revealing physical addresses. The process is reversed for clients on the corporate LAN seeking to dial up remote destinations.

In Figure 15 below, the IP addresses received at the NAT Server for Servers #1, #2 and the ANG are translated into the real IP addresses of the destination servers.

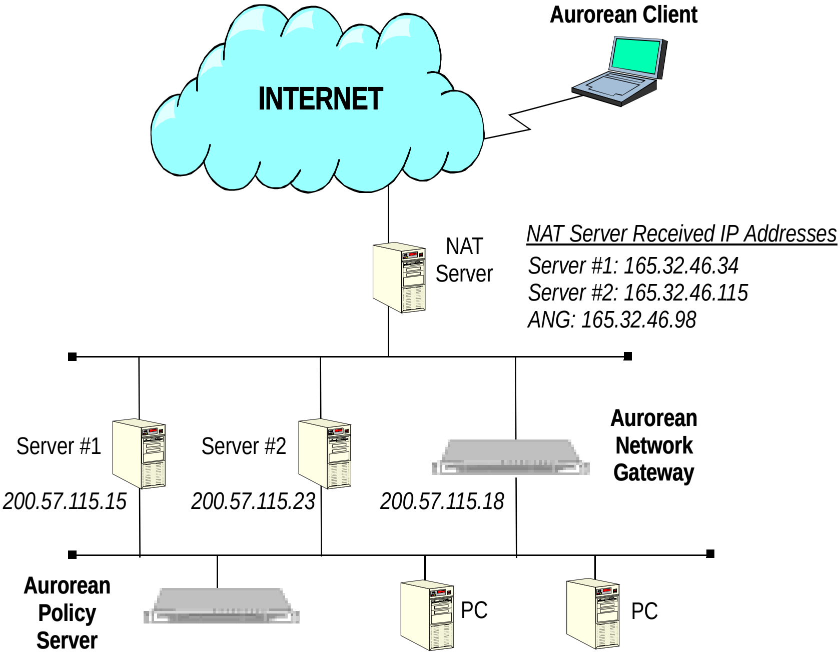


Figure 15 Aurorean Virtual Network's NAT Server Feature

NOTE

Aurorean's NAT Server implementation cannot be employed as a *client* NAT where, for example, it operates within a cable modem / ISP topology. Aurorean's NAT Server implementation is *server*-centric.

Site-to-Site Tunnels

Aurorean site-to-site tunnels optimize service between remote offices and their remotely linked corporate LANs. This configuration is similar to a remote access Aurorean connection in the sense that both configurations originate tunnels from an ANG and terminate the tunnel at a remote site. The site-to-site tunnel configuration *differs* from the typical ANG model in the sense that the remote server and tunnel must be configured with several network values which identify the remote server to the local ANG. Figure 16 displays two site-to-site configurations of Regional Offices A and B connected to a local ANG and both remote offices connected together, as well as a remote access connection into Corporate Headquarters.

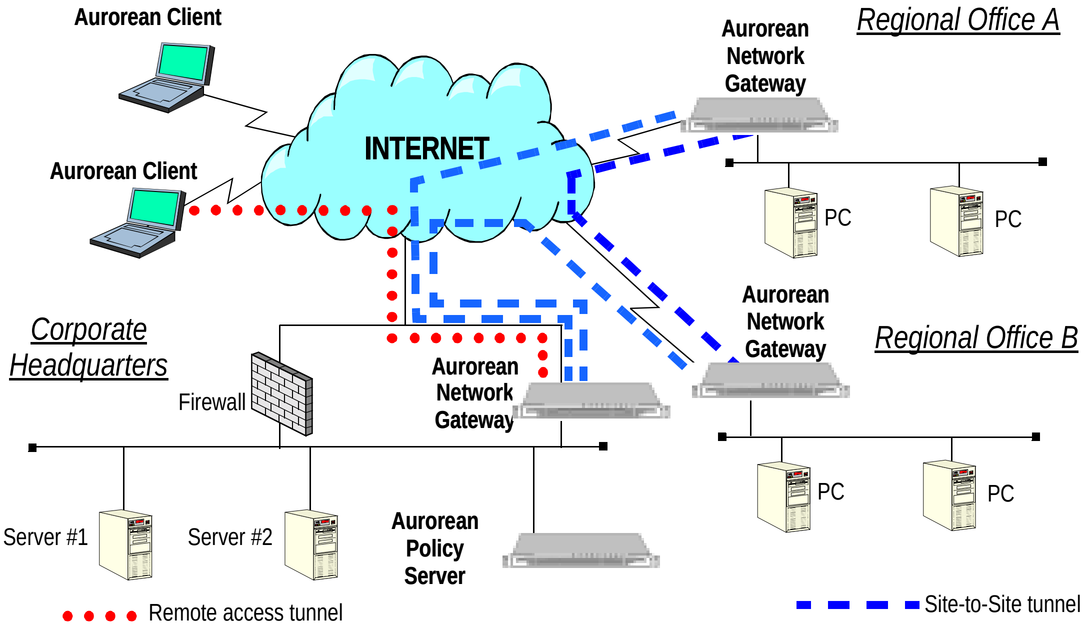


Figure 16 Site-to-Site Configuration

When corporate networks are linked via one or more tunnels, users can utilize applications over these LANs simply by choosing a network-supported program or by using Windows Explorer to find a destination server. Using Aurorean Client to dial up a remote connection is not required.

Remote Aurorean site-to-site connections are set up by first adding a remote ANG to an existing ANG configuration, then adding the tunnel itself. This is done by configuring a *user* on that server with the following values: an IP address or Fully Qualified Domain Name (FQDN) for the server, a user name and password, and a tunnel protocol (either IPSec or PPTP). These are all the values required to make the connection. We recommend that you enable Intelligent Client Routing on both Aurorean Virtual Network Network Gateways so clients accessing the tunnel remotely or locally can access clients on the far end of the network.

✓ NOTE

Enable at least one routing protocol (RIPv1, RIPv2 or OSPF) on the ANG. Refer to Chapter 3 for instructions.

Refer to “Adding a Remote Server” on page 68 to configure a site-to-site tunnel.

AutoLink Recovery

Auto LinkRecovery (ALR) extends the fault isolation and recovery capabilities of the Aurorean Client to include automatic fail-over to a backup Aurorean Virtual Network system in the event of a service outage or VPN hardware failure.

To support ALR, a second Aurorean Virtual Network system APS, ANG, and RiverMaster management application) is required. The secondary Aurorean Virtual Network system operates in parallel but independently of the primary Aurorean Virtual Network system. Each system must be located on the same corporate network, but can be physically situated at different sites, to support disaster recovery, as shown in Figure 17. For more detailed information, refer to “Viewing Aurorean Alternate Address Information” on page 42.

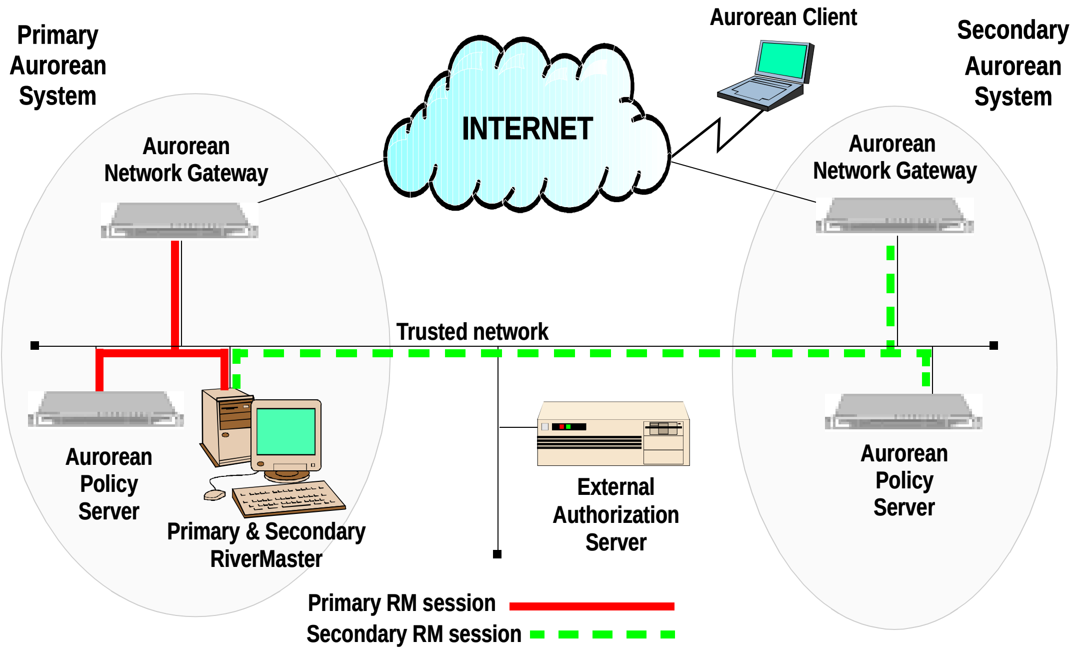


Figure 17 Auto Link Recovery Architecture

If the primary Aurorean Virtual Network system fails or is unreachable due to Internet congestion, corporate ISP outage, or router malfunction, the secondary Aurorean Virtual Network system provides continued VPN service to remote users and branch offices.

From the standpoint of network topology, both Aurorean Virtual Network systems share the same Management domain name although they are physically discrete. Also, a RiverMaster management application serving each Aurorean Virtual Network system is accessible at and operates from a single Windows NT/2000 computer. The Aurorean Virtual Network system pairs can handle authentication through a shared database if an external service such as RADIUS or SecurID is used. ALR also supports Enterasys authentication via the APS database although this requires that user information be manually replicated in each Aurorean Virtual Network system. For more detailed information, refer to the *AutoLink Recovery* Application Note.

General Aurorean Network Gateway Settings

General network settings for the ANG include:

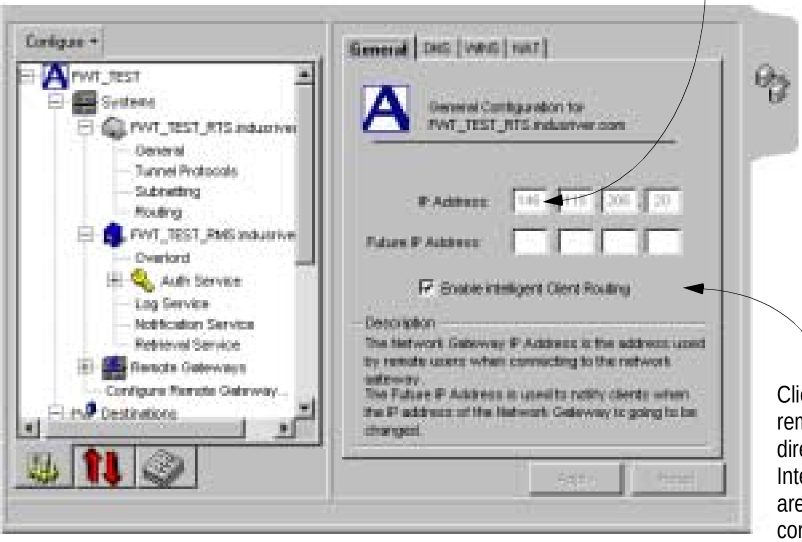
- The current and possible future IP addresses for the server.
- Enabling Aurorean Virtual Network's Intelligent Client Routing feature which provides you with a measure of control over a Aurorean Client's access to the Internet.
- Addresses for the Domain Name System (DNS), Windows Internet Name Service (WINS), and Network Address Translation (NAT) servers used by remote clients for name resolution.

To set general network settings for the ANG, perform the following steps:

1. Open the Configuration pullout.
2. In the list of Aurorean devices, expand the tree list under Servers (click the + symbol).
3. Expand the tree list under the name of your ANG.
4. Click on General to display the general network settings tab pages.

   A sample General settings window appears as shown in Figure 18. The IP Address field is read-only and displays an address assigned to the ANG during installation. If the ANG is equipped with a single Ethernet interface, this field shows the address of the Trusted port. If the ANG is equipped with dual Ethernet interfaces, this field shows the address of the External port.

The Aurorean Network Gateway IP address is set when the servers are installed and displayed here as read-only



General Configuration for FWT_TEST_RTS.indusriver.com

IP Address: 146 . 115 . 206 . 20

Future IP Address:

☑ Enable Intelligent Client Routing

Description

The Network Gateway IP Address is the address used by remote users when connecting to the network gateway.
The Future IP Address is used to notify clients when the IP address of the Network Gateway is going to be changed.

Click here to allow remote users to directly browse the Internet while they are tunneled into the corporate network

Figure 18 General Aurorean Network Gateway Settings

5 If you plan to change the Aurorean Network Gateway’s IP address in the future, enter the new address in the Future IP Address field; otherwise, leave this field blank and continue with the next step.

When you build a custom Aurorean Client installation kit for your remote users (as described in Chapter 6), the ANG’s IP address is saved as part of the kit. Aurorean Client needs this address to locate the ANG across the Internet and create a tunnel. If you enter an IP address in the Future IP Address field, the kit will contain both IP addresses that appear on this pullout. If Aurorean Client cannot locate a ANG by first using the standard IP address, it will automatically use the future IP address. If connecting to this address is unsuccessful, a user can enter an IP address in the Alternate Tunnel Server IP address field in Aurorean Client. Refer to the *Aurorean Client User’s Guide* for more information.

6 To allow remote users to browse the Internet directly while they are tunneled into the corporate network, place a check next to Enable Intelligent Client Routing on the General page.

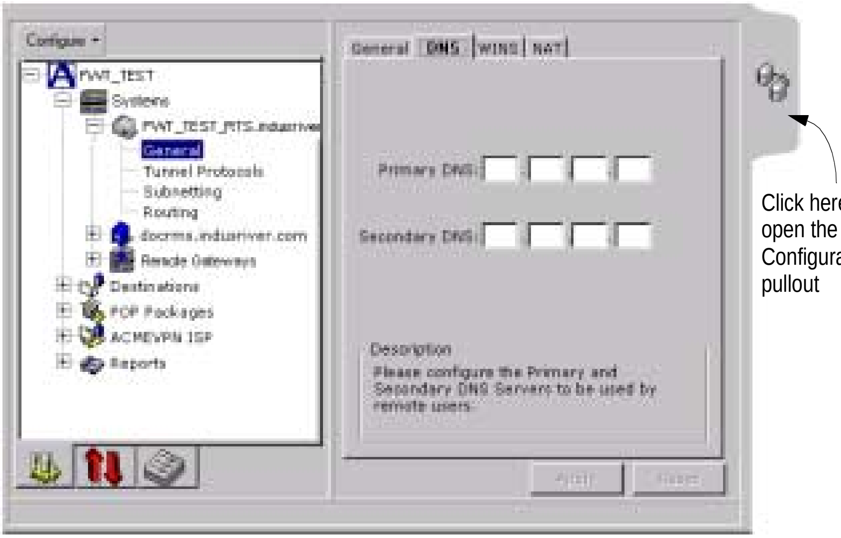
For more information on Aurorean Virtual Network's Intelligent Client Routing feature, refer to "Intelligent Client Routing" on page 31.

NOTE

The Reset button returns any altered values to their earlier setting.

7 Click the DNS tab.

The DNS server addresses tab page appears as shown in Figure 19.



Please configure the Primary and Secondary DNS Servers to be used by remote users.

Click here to open the Configuration pullout

Figure 19 DNS Server Addresses

8 In the Primary DNS and Secondary DNS fields, enter the IP addresses of DNS servers on your network.

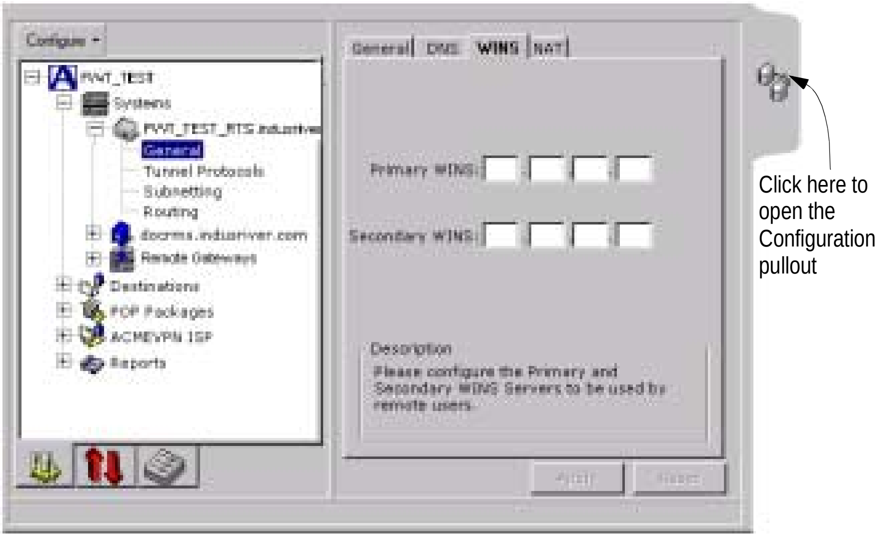
You must identify a primary DNS server; the secondary DNS server is optional. The primary and secondary labels indicate the search order (primary first and then secondary). Select DNS servers that can resolve the names of network devices that remote clients must access.

CAUTION

Not specifying a value for both primary and secondary DNS and WINS servers may cause connection problems on networks with Windows NT clients. To avoid this possibility, enter the IP address used on your primary DNS server in all DNS/WINS fields even if you do not have a secondary DNS or primary or secondary WINS server installed on your network.

9 Click the WINS tab.

The tab page for Windows Internet Name Service (WINS) server addresses appears as shown in Figure 19.



Primary WINS: □ □ □ □

Secondary WINS: □ □ □ □

Description

Please configure the Primary and Secondary WINS Servers to be used by remote users.

Click here to open the Configuration pullout

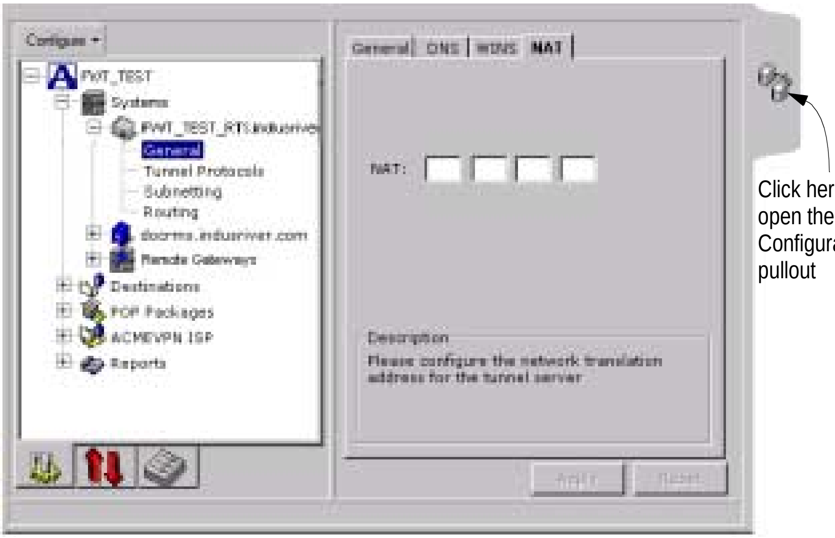
Figure 20 WINS Server Addresses

10 In the Primary WINS and Secondary WINS fields, enter the IP addresses of WINS servers on your network.

If your remote clients use standard Microsoft Dial-Up Networking (DUN) on the corporate network, you must complete these fields to enable browsing and communication with other devices in the Network Neighborhood.

11 Click the NAT tab.

The tab page for the Network Address Translation (NAT) server address appears as shown in Figure 21.



NAT:

Description
Please configure the network translation address for the tunnel server

Click here to open the Configuration pullout

Figure 21 NAT Server Address

12 In the NAT field, enter the IP Address of the NAT server on your network.

The IP address you enter here is the address that Aurorean users will receive in the installation kit as their destination address - the alias external IP address of the ANG.

NOTE

You must configure an IP address on your NAT Server that correlates with the alias IP address you set here.

13 Click Apply to save your changes.

To return the parameters to their original settings without saving your changes, click Reset.

14 Do one of the following:

– If you are setting up your Aurorean Virtual Network for the first time, continue with the next subsection to configure additional ANG network settings.

– If you are finished with the ANG network configuration and you want to put the new network settings into effect, no additional work is required.

Viewing Aurorean Alternate Address Information

The Aurorean Alternate Address Info window displays IP addresses of the alternate APS and ANG systems, as well as those of the primary system.

To invoke the display, perform the following steps:

1 Open the Configuration pullout.

2 Click the arrow on the Configure toolbar item at the top left edge of the pullout.

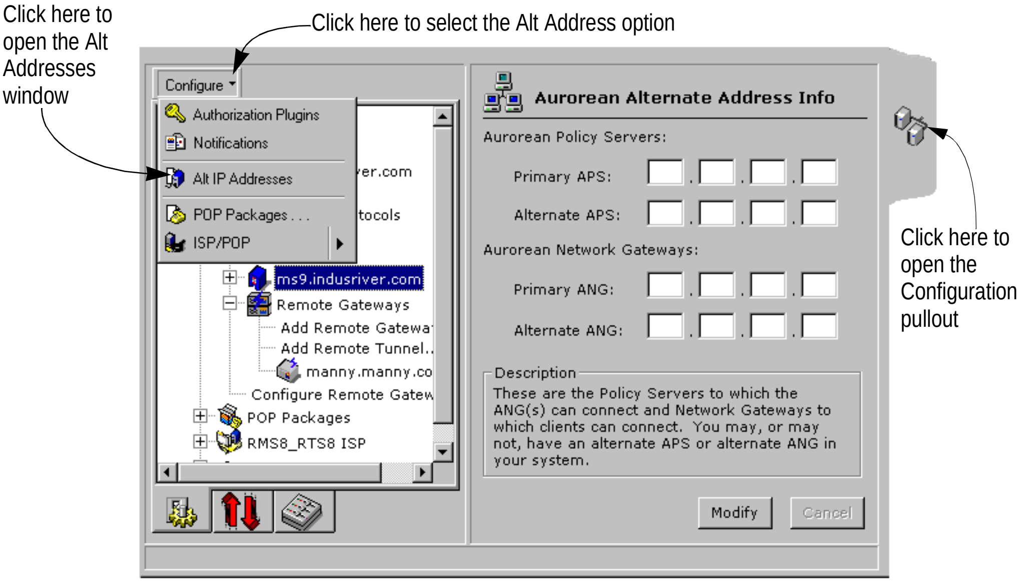
3 Choose Alt IP Addresses as shown in Figure 22.

The Aurorean Alternate Address Info window appears as shown in Figure 22.

4 View the ANG and APS Primary and Secondary (if previously configured) IP addresses.

NOTE

Primary addresses cannot be modified in this window.



Click here to open the Alt Addresses window

Click here to select the Alt Address option

Click here to open the Configuration pullout

Aurorean Alternate Address Info

Aurorean Policy Servers:

Primary APS: [ ].[ ].[ ].[ ]

Alternate APS: [ ].[ ].[ ].[ ]

Aurorean Network Gateways:

Primary ANG: [ ].[ ].[ ].[ ]

Alternate ANG: [ ].[ ].[ ].[ ]

Description

These are the Policy Servers to which the ANG(s) can connect and Network Gateways to which clients can connect. You may, or may not, have an alternate APS or alternate ANG in your system.

Figure 22 Aurorean Alternate Address Info Window

5 If you want to change either the ANG or APS Alternate IP address, click Modify, enter a value and click Update.

Tunnel Protocols

The ANG supports two tunnel protocols:

- ❒ Point-to-Point Tunneling Protocol (PPTP) developed by Microsoft, 3Com and others that uses Point-to-Point (PPP) protocol and Generic Routing Encapsulation (GRE) to route packets through the Internet.
- ❒ IP Security (IPSec) protocol developed by the Internet Engineering Task Force (IETF) that adds security extensions for encryption and message authentication to IP protocol.

For each tunnel protocol, you can configure authentication, encryption, and compression parameters. To set tunnel protocol parameters, perform the following steps:

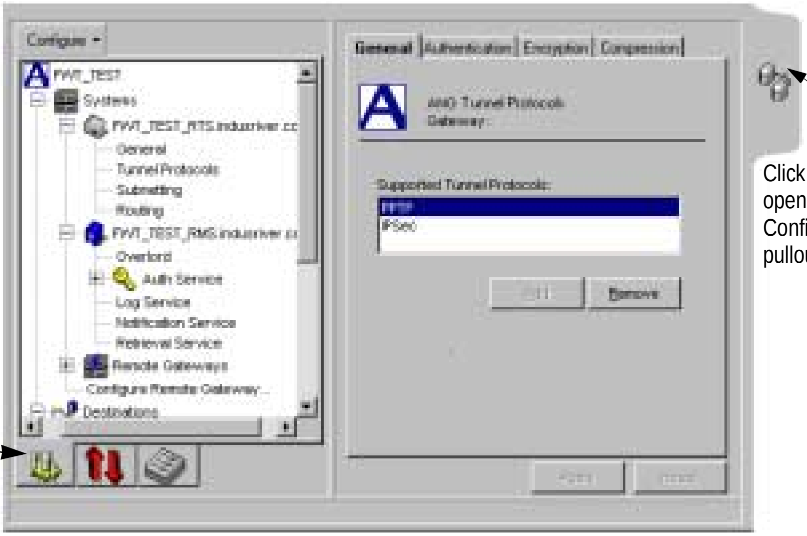
1 Open the Configuration pullout.

2 In the list of Aurorean devices, expand the tree list under Servers (click the + symbol).

3 Expand the tree list under the name of your ANG.

4 Click on Tunnel Protocols to display PPTP and IPSec protocol tab pages.

The Tunnel Protocols window appears as shown in Figure 23.



Click here to access the Gateway configuration windows

Click here to open the Configuration pullout

Figure 23 Tunnel Protocol General Settings

5 If you want to prevent remote clients from using one of the tunnel protocols, select the protocol and click Remove.

By default, PPTP and IPSec are both enabled for client use. You normally control protocol usage on a per group basis by selecting the protocol when you assign group policies (refer to Chapter 6 for instructions). If you want to globally disable a protocol, you can remove it from this list. If you have removed a protocol and want to reinstall it, click Add once and when the highlighted tunnel protocol pops up, click Add again. You are not required to click Apply.

6. Click the Authentication tab.

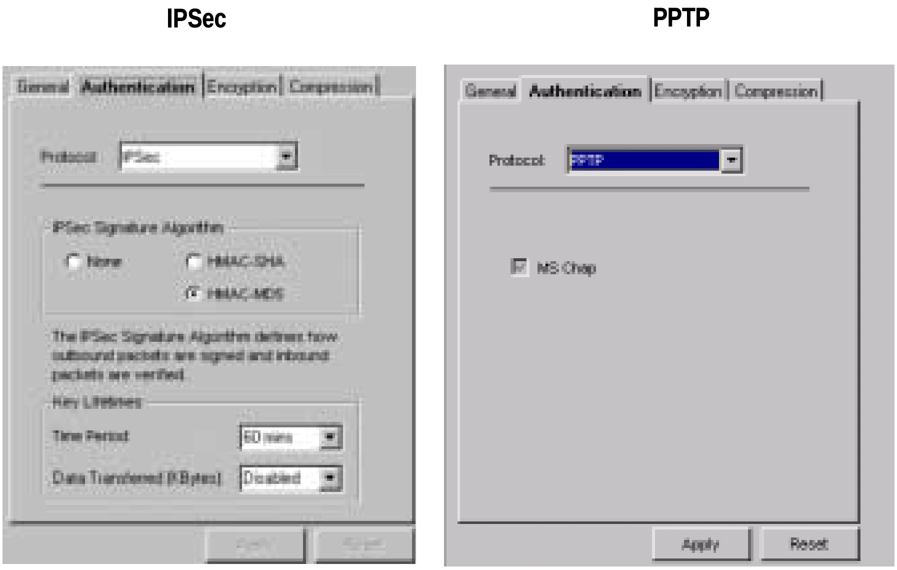
   Figure 24 shows the authentication parameters available for each tunnel protocol.

7. Do one of the following:

   – Choose IPSec from the Protocol pull down menu.

     - Use the information in Table 2 to select the IPSec Signature Algorithm that determines how IPSec packets exchanged between the ANG and Aurorean users are signed and verified.
     - Set the Key Lifetimes Time Period and Data Transferred value. The default values are 60 minutes for Time Period and Disabled for Data Transferred. Refer to Table 2 to select the Time Period and Data Transferred values which set how long the key lifetime should last in terms of time elapsed or kilobytes amassed.
     - Click Apply.

   – For PPTP, no additional work is required. Unlike IPSec, PPTP does not authenticate individual packets; instead, PPTP relies on user authentication using MS-CHAP. After the remote user is authenticated, all PPTP packets are allowed access.



IPSec

Protocol: IPSec

IPSec Signature Algorithm

○ None ○ HMAC-SHA ● HMAC-MD5

The IPSec Signature Algorithm defines how outbound packets are signed and inbound packets are verified.

Key Lifetimes

Time Period: 60 mins

Data Transferred (KBytes): Disabled

PPTP

Protocol: PPTP

☑ MS-Chap

Figure 24 Tunnel Protocol Authentication Settings

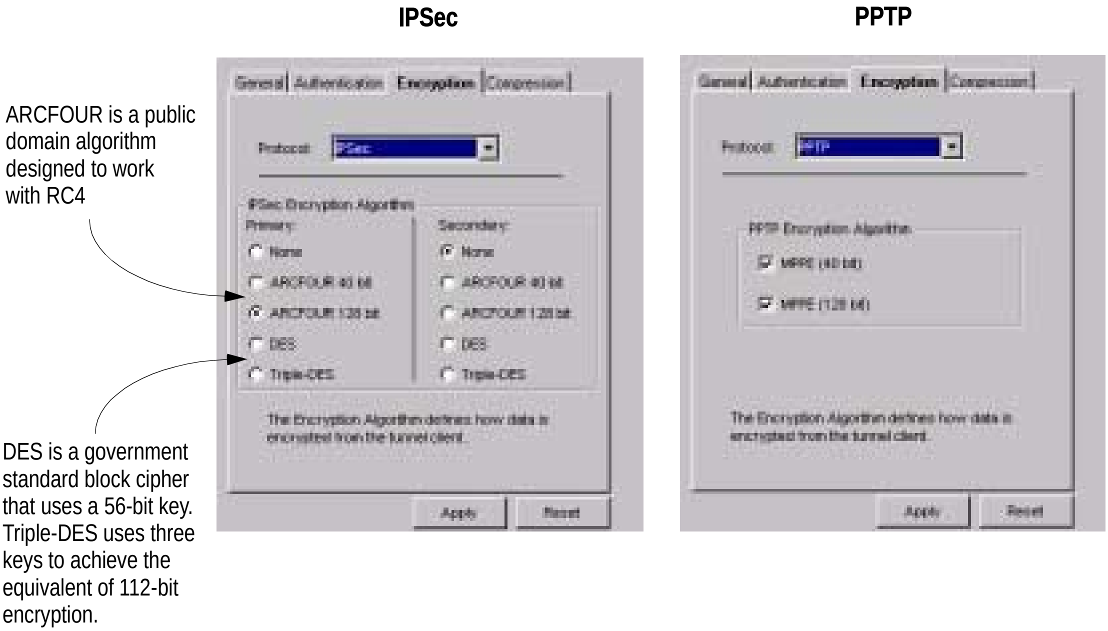
Table 2 IPSec Authentication Parameters

Parameter	**Explanation**
None	Disables the Signature Algorithm for IPSec packets; individual packets are no longer signed and verified during transmission.
HMAC-SHA	Enables hashing message authentication codes (HMAC) that are generated using the SHA cryptographic hashing function. HMAC-SHA is generally regarded as stronger, more secure cryptographic function than HMAC-MD5.
HMAC-MD5	Enables hashing message authentication codes (HMAC) that are generated using the Rivest MD5 message digest algorithm hashing function. While not as strong cryptographically as HMAC-SHA, HMAC-MD5 provides better performance.
Time Period	Interval after which a new key is generated.
Data Transferred	Lifetime volume (in kilobytes) of the key after which a new key is generated.

8 Click the Encryption tab.

9 Do one of the following:

- To set IPSec encryption parameters, choose **IPSec** from the Protocol menu. IPSec encryption parameters are shown in Figure 25. Select the IPSec Encryption Algorithm that determines how IPSec packets exchanged between the ANG and Aurorean Client remote users are encrypted.
- To set PPTP encryption parameters, choose **PPTP** from the Protocol menu. PPTP encryption parameters are shown in Figure 25. Select the Microsoft Point-to-Point Encryption (MPPE) algorithm that determines how PPTP packets exchanged between the ANG and Aurorean remote users are encrypted.



IPSec

Protocol: IPSec

IPSec Encryption Algorithms

Primary:
- ○ None
- ○ ARCFOUR 40 bit
- ● ARCFOUR 128 bit
- ○ DES
- ○ Triple-DES

Secondary:
- ● None
- ○ ARCFOUR 40 bit
- ○ ARCFOUR 128 bit
- ○ DES
- ○ Triple-DES

The Encryption Algorithm defines how data is encrypted from the tunnel client.

PPTP

Protocol: PPTP

PPTP Encryption Algorithm
- ☑ MPPE (40 bit)
- ☑ MPPE (128 bit)

The Encryption Algorithm defines how data is encrypted from the tunnel client.

ARCFOUR is a public domain algorithm designed to work with RC4

DES is a government standard block cipher that uses a 56-bit key. Triple-DES uses three keys to achieve the equivalent of 112-bit encryption.

Figure 25 Tunnel Protocol Encryption Settings

Table 3 Encryption Parameters

Tunnel Protocol	Parameter	Explanation
IPSec	None	Disables encryption on the tunnel; because this results in a less secure connection, this setting is not recommended.
	ARCFOUR 40 bit	Enables a 40-bit key public domain algorithm that is designed to work with Rivest Cipher 4 (RC4), a stream-based cipher method that supports both 40-bit and 128-bit keys. Using RC4, data packets can be encrypted as they are received instead of in blocks.
	ARCFOUR 128 bit	Enables a 128-bit key version of ARCFOUR (described above).
	DES	Enables Data Encryption Standard (DES), a block cipher method that uses 56-bit keys. Using DES, data is encrypted in fixed-size blocks and packets are padded to become a multiple of the block size.
	Triple-DES	Enables a version of DES (described above) that employs a DES encryption with one key, a decryption with a second key, and then another encryption with a third key. The result is equivalent to DES with a 112-bit key.
PPTP	MPPE (40 bit)	Enables 40-bit key Microsoft Point-to-Point Encryption (MPPE) which generates a key based on a hash of the user’s password and invokes RC4 encryption. This type of encryption is supported by Windows 95/98/NT/2000/ME computers without any additional software.
	MPPE (128 bit)	Enables 128-bit key MPPE on the tunnel. To support 128-bit keys, the Aurorean computer must receive a 128-bit encryption upgrade available from Microsoft. This upgrade may not be available to users outside the U.S.

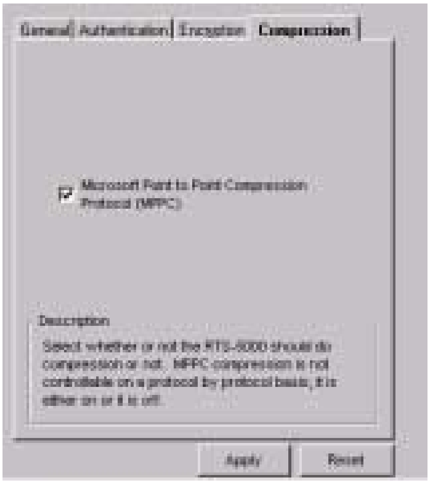
10 Click the Compression tab.

11 Enable or disable MPPC as required.

For both IPSec and PPTP protocols, Microsoft Point-to-Point Compression (MPPC) is currently the only compression technique supported by the ANG. By default MPPC compression is enabled for both protocols.

NOTE

Compression settings are applied automatically to both tunnel protocols. That is, disabling compression on IPSec also disables compression on PPTP.



☑ Microsoft Point to Point Compression Protocol (MPPC)

Description

Select whether or not the RTS-5000 should do compression or not. MPPC compression is not controllable on a protocol by protocol basis, it is either on or it is off.

Figure 26 Tunnel Protocol Compression Settings

12 Click Apply to save your changes.

To return the parameters to their original settings without saving your changes, click Reset.

13 Do one of the following:

- If you are setting up your Aurorean Virtual Network for the first time, continue with the next subsection to configure additional ANG network settings.
- If you are finished with the ANG network configuration and you want to put the new network settings into effect, no additional work is required.

Virtual Subnetting

Virtual subnets fall into two categories:

❐ IP subnets that serve as IP address pools for allocation to remote clients when they connect.

❐ An IPX network number that is shared by all remote clients when they connect and use IPX protocol to access Novell NetWare servers.

IP Subnetting

To set up virtual subnets of IP addresses to allocate to remote users, perform the following steps:

1 Open the Configuration pullout.

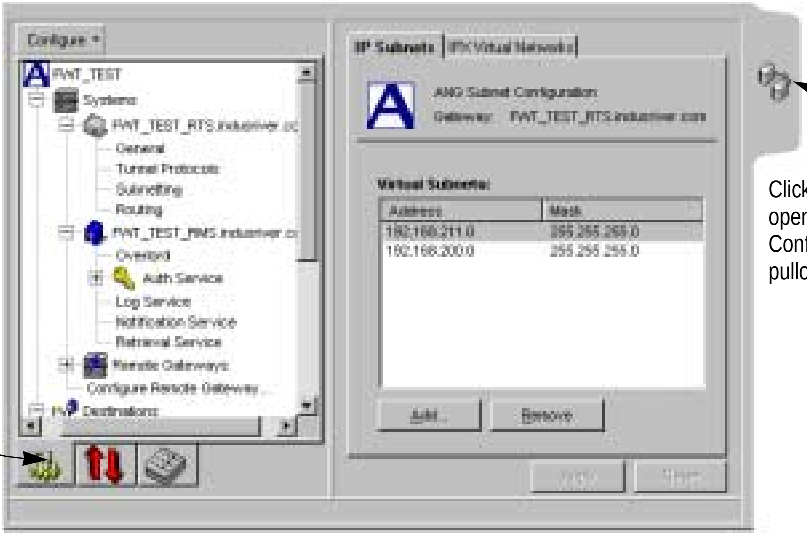
2 In the list of Aurorean devices, expand the tree list under Servers (click the + symbol).

3 Expand the tree list under the name of your ANG.

4 Click on Subnetting to display IP and IPX subnet tab pages.

5 Click the IP Subnets tab if it is not already displayed.

A sample IP subnet window is shown in Figure 27.



ANG Subnet Configuration
Gateway: FWT_TEST_RTS.indusriver.com

Virtual Subnets:

Address	Mask
192.168.211.0	255.255.255.0
192.168.200.0	255.255.255.0

Click here to access the Gateway configuration windows

Click here to open the Configuration pullout

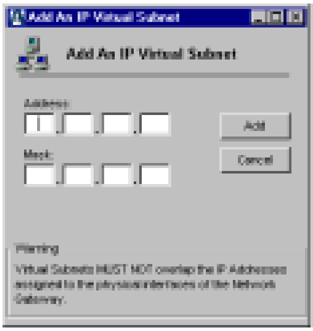
Figure 27 IP Subnet Configuration for Remote Clients

NOTE

Click Remove to delete any configured virtual subnets.

6 Click Add.

The Add An IP Virtual Subnet window appears as seen in Figure 28.



Warning

Virtual Subnets MUST NOT overlap the IP Addresses assigned to the physical interfaces of the Network Gateway.

Figure 28 Adding An IP Virtual Subnet

7. Enter the starting address of the subnet in the Address fields.

   You can use actual IP addresses from your network or non-routable IP address ranges (such as 192.168.x.x for a Class C network).

8. Enter a subnet mask to define the subnet range in the Mask field.

9. Do one of the following:
   - Click Add to add the new virtual subnet.
   - Click Cancel to close the window without saving your changes.

10. Repeat Step 6 through Step 9 for each virtual subnet you require.

11. Click Apply to save your changes.

    To return the parameters to their original settings without saving your changes, click Reset.

12. Do one of the following:
    - If you are setting up your Aurorean Virtual Network for the first time, continue with the next subsection to configure additional ANG network settings.
    - If you are finished with the ANG network configuration and you want to put the new network settings into effect, no additional work is required.

IPX Virtual Networks

To set up a single IPX network number to allocate to remote users, perform the following steps:

1. Open the Configuration pullout.

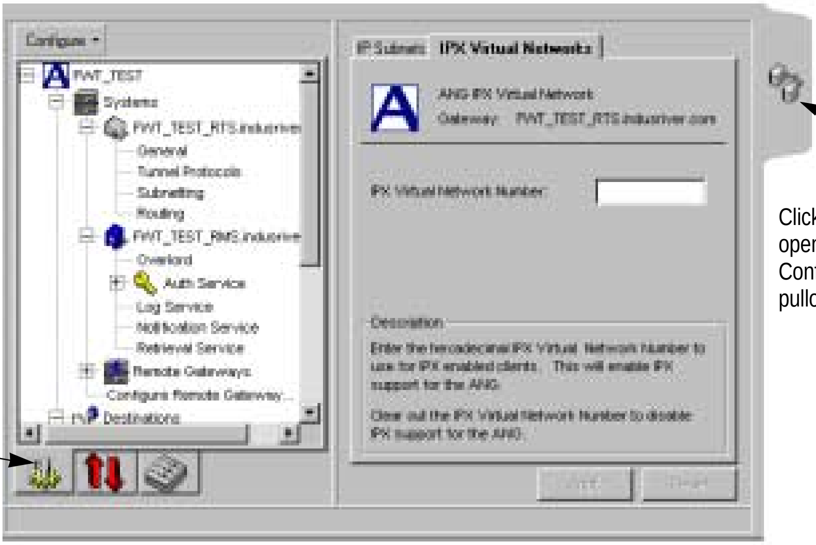
2. In the list of Aurorean devices, expand the tree list under Servers (click the + symbol).

3. Expand the tree list under the name of your ANG.

4. Click on Subnetting to display IP and IPX subnet tab pages.

5. Click the IP Virtual Networks tab if it is not already displayed.

   A sample IPX virtual networks window is shown in Figure 29.



Enter the hexadecimal IPX Virtual Network Number to use for IPX enabled clients. This will enable IPX support for the ANG.

Clear out the IPX Virtual Network Number to disable IPX support for the ANG.

Click here to access the Gateway configuration windows

Click here to open the Configuration pullout

Figure 29 IPX Subnet Configuration for Remote Clients

6 In the IPX Virtual Network Number field, enter an IPX network number to be used by all remote clients. This number must be unique.

The network number must be between 1 and 8 hexadecimal digits (1 to FFFFFFFD). This network number will be attached to all IPX frames received from remote clients.

NOTE

Zero (0) and FFFFFFFF addresses are invalid due to NetWare restrictions. FFFFFFFE is reserved for the default route.

7 Click Apply to save your changes.

To return the parameters to their original settings without saving your changes, click Reset.

8 Do one of the following:

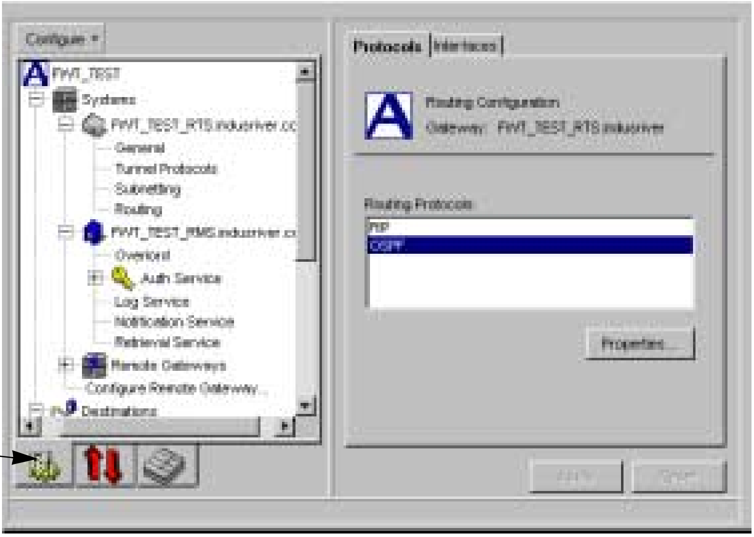
- If you are setting up your Aurorean Virtual Network for the first time, continue with the next subsection to configure additional ANG network settings.
- If no additional ANG network configuration is required and you want to put the new network settings into effect, reset the ANG.

Routing

Configuring the routing behavior of the ANG consists of two general steps:

❒ Setting parameters for the two routing protocols supported, RIP and OSPF.

❒ Selecting routing protocols for each ANG Ethernet interface.



Click here to access the Gateway configuration windows

Click here to open the Configuration pullout

Figure 30 Aurorean Network Gateway Routing Configuration

Setting Routing Protocol Parameters

To access RIP and OSPF parameters for the ANG, perform the following steps:

1 Open the Configuration pullout.

2 In the list of Aurorean devices, expand the tree list under Servers (click the + symbol).

3 Expand the tree list under the name of your ANG.

4 Click on Routing to display the routing parameter tab pages.

5 Click on the Protocols tab to display protocol parameters for RIP and OSPF.

6 Do one of the following:

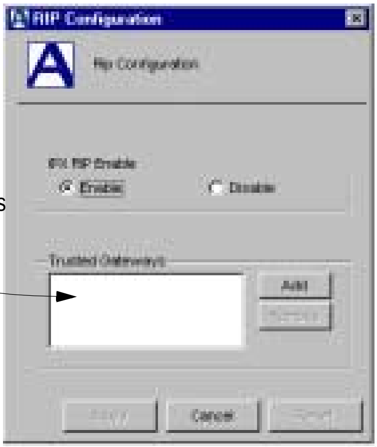
- To set RIP parameters, choose RIP from the Routing Protocols menu and click Properties; refer to the next section “Setting RIP Properties” for additional instructions.
- To set OSPF parameters, choose OSPF from the Routing Protocols menu and click Properties; refer to “Setting OSPF Properties” on page 57 for additional instructions.

Setting RIP Properties

To configure RIP properties for the ANG, perform the following steps:

1 Perform the steps in the previous section to access RIP properties.

The RIP Configuration window should appear as shown in Figure 31.



If this list is blank, the Aurorean Network Gateway accepts RIP updates from all routers on the subnet. You can limit the amount of updates that the Aurorean Network Gateway will accept by specifying individual routers in this list.

Figure 31 RIP Routing Protocol Configuration

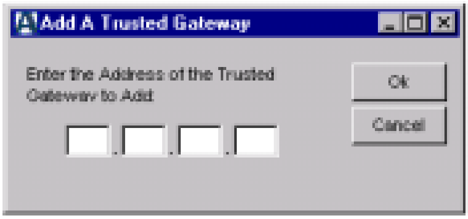
2 To turn on RIP for IPX packets, click Enable under IPX RIP Enable; otherwise, continue with the next step.

3 Do one of the following:

– To allow the ANG to accept RIP updates from all routers on the same subnet, no further work is required. Skip to Step 6.

– To configure “trusted” individual routers to supply RIP updates to the ANG, click Add and continue with the next step.

The Add A Trusted Gateway window appears as shown in Figure 32.



Enter the Address of the Trusted Gateway to Add

Figure 32 Adding A Trusted Gateway for RIP

4 In the Address field, type the address for the router that the ANG will accept updates from and click Add.

You can later modify this address or delete it using the Modify and Remove buttons.

5 Repeat Step 3 and Step 4 for each gateway required.

6 Do one of the following:

- Click Apply to save your changes.
- Click Cancel to close the window without saving your changes.
- Click Reset to return the RIP parameters to their default settings.

Setting OSPF Properties

Using the RiverMaster, you can define the following OSPF parameters:

- ❐ Area ID shared by the routers and the ANG.
- ❐ Router ID that identifies the ANG to other devices in the OSPF area. The default value for this address is the IP address assigned to the Trusted interface on the ANG.
- ❐ Authentication algorithm used to accept or reject routing table updates from other routers.

To route packets for remote clients using OSPF, the ANG also uses a set of fixed operating parameters. Table 4 lists these fixed OSPF parameters, which use common default values and cannot be changed.

Table 4 Fixed OSPF Parameters

Parameter	Meaning	Fixed Value
Preference	Determines how OSPF routes compete with routes from other protocols (such as RIP) in the ANG’s routing table. The route with the lowest preference value is selected.	150
Cost	Used when exporting a non-OSPF route from the ANG’s routing table into OSPF as an autonomous system (AS).	1
Type	Indicates which type of autonomous systems that routes exported from the ANG’s routing table become.	Type 1 AS
AS Export Interval	Specifies how often autonomous system link advertisements are generated and exported.	Once per second

Table 4 Fixed OSPF Parameters

Parameter	Meaning	Fixed Value
AS Export Limit	Specifies how many autonomous systems are generated and exported each time.	100
Interface Priority	Determines the ANG's priority for becoming the designated router in the area.	0 (the ANG cannot be the designated router)

To configure OSPF properties for the ANG, perform the following steps.

1. Perform the steps in "Setting Routing Protocol Parameters" on page 55 to access OSPF properties.

   The OSPF Configuration window appears as shown in Figure 33.

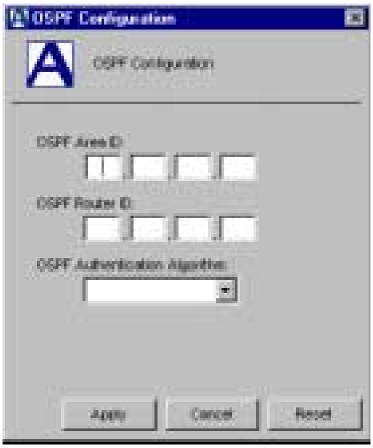


Figure 33 OSPF Routing Protocol Configuration

2. Type the area ID shared by the ANG and routers within the subnet in the OSPF Area ID fields.

3. Type the IP address for the Trusted interface in the OSPF Router ID fields.

4 From the OSPF Authentication Algorithm menu, choose the authentication algorithm used by routers on your network.

If the routers on your network do not require passwords to accept OSPF updates, set the algorithm to None and continue with the next step.

5 Do one of the following:

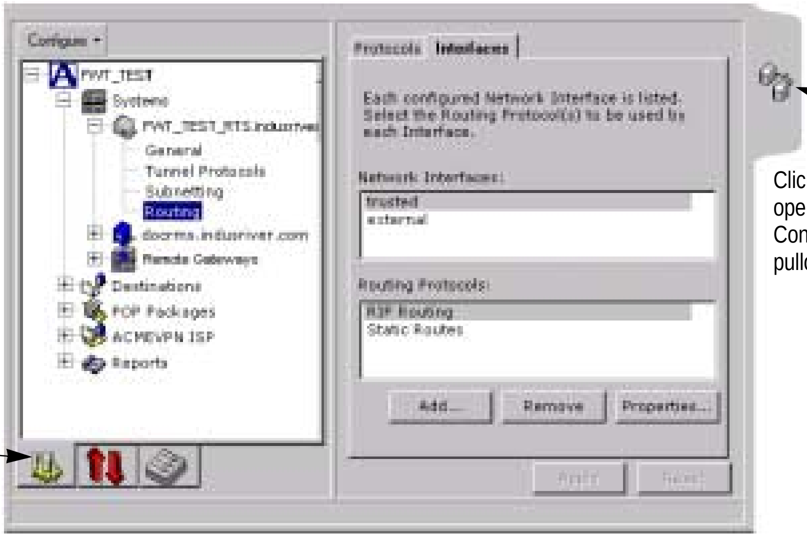
- Click Apply to save your changes.
- Click Cancel to close the window without saving your changes.
- Click Reset to the return the OSPF properties to their default settings.

Routing Interfaces

The ANG is equipped with two Ethernet interfaces:

❒ The *Trusted* interface should be connected to a protected network segment (one behind a firewall or router that offers protection against unauthorized access). Typically, you should enable a routing protocol (RIP, OSPF, or both) on the Trusted interface so that the ANG can advertise to other devices that its virtual subnets are reachable to the corporate network.

❒ The *External* interface can be connected to a network segment that resides outside a firewall and offers unfiltered access to the Internet. You must create a static route between the External interface and the router that serves as the gateway to the Internet. You cannot enable RIP or OSPF on this interface.



Each configured Network Interface is listed. Select the Routing Protocol(s) to be used by each Interface.

Network Interfaces:

trusted
external

Routing Protocols:

RIP Routing
Static Routes

Click here to access the Gateway configuration windows

Click here to open the Configuration pullout

Figure 34 Aurorean Network Gateway Routing Interface Configuration

Adding or Removing a Routing Protocol for an Interface

To add or remove a routing protocol from an interface, perform the following steps:

1. Open the Configuration pullout.
2. In the list of Aurorean devices, expand the tree list under Servers (click the + symbol).
3. Expand the tree list under the name of your ANG.
4. Click on Routing to display the routing parameter tab pages.
5. Click on the Interfaces tab to display the configuration for each ANG network interface.

6 Select the interface (Trusted or External) from the list under Network Interfaces.

The protocols already enabled for this interface appear in the Routing Protocols list.

7 Do one of the following:

- To add a protocol to the trusted interface, click Add and continue with the next step.
- To remove a protocol, select the protocol from the Routing Protocols list and click Remove. Skip to Step 10.

8 When the Add an Interface Routing Protocol window appears as shown in Figure 35, select a routing protocol and click Add.

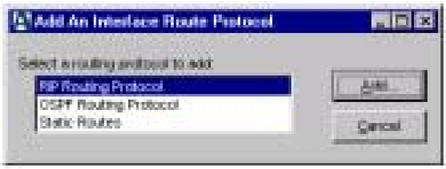


Figure 35 Adding a Routing Protocol

NOTE

For the External interface, you can only add or remove static routing. Because the External interface is optimized for tunnel protocols only, you cannot use RIP or OSPF on this interface.

9 Do one of the following:

- If you are adding RIP to the interface, perform the steps in “Configuring RIP for the Interface” on page 62.
- If you are adding OSPF to the interface, perform the steps in “Configuring OSPF on an Interface” on page 64.
- If you are adding a static route to the interface, perform the steps in “Creating Static Routes” on page 65.

10 Do one of the following:

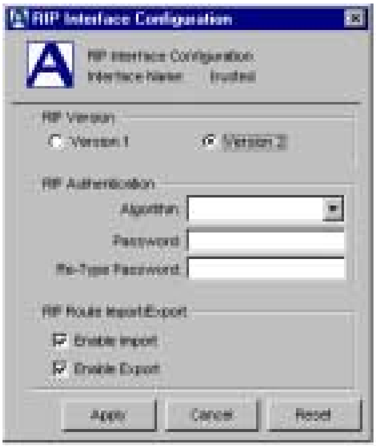
- Click Apply to save the routing protocol configuration changes.
- Click Reset to the return the interface’s protocol configuration to its original setting.

Configuring RIP for the Interface

To configure RIP on an interface, perform the following steps:

1 Add RIP as described in the previous section or select RIP from the Routing Protocols list and click Properties.

The RIP Interface Configuration window appears as shown in Figure 36.



RIP Interface Configuration

RIP Interface Configuration
Interface Name: trusted

RIP Version
○ Version 1 ● Version 2

RIP Authentication
Algorithm: [▾]
Password: [ ]
Re-Type Password: [ ]

RIP Route Import/Export
☑ Enable Import
☑ Enable Export

These values are used to authenticate RIP updates from routers on the network

Figure 36 Routing Interfaces Configuration - RIP

2 Choose the version of RIP to use on this interface.

RIP Version 1 uses IP broadcast packets for periodic announcements of reachable subnets. RIP Version 2 is an enhanced version of RIP that uses IP multicast packets for announcements.

3 In the RIP Authentication fields, choose the algorithm used by routers on your network.

If the routers on your network do not require passwords to accept RIP updates, set the algorithm to None and skip to Step 7.

☑ NOTE

RIP update authentication is only supported by RIP Version 2. If the routers on your network only support RIP Version 1, you cannot enter values in the RIP Authentication fields. Refer to “Configuring RIP for the Interface” on page 62 for instructions on selecting the version of RIP used on your network.

4 Type the RIP authentication password used by routers on your network in the Password field.

RIP authentication passwords are used by routers to determine if they should accept updated routing information sent from another router. If your routers do not authenticate updates, leave this field blank and skip to Step 2.

5 Type the same password in the Re-Type Password field exactly as you entered it in Step 4.

6 Set the RIP Route Importing/Exporting options as follows:

- To allow the ANG interface to learn new routes, place a check next to Enable Import. If you enabled the Intelligent Client Routing feature, you should turn on Enable Import to allow the ANG to pass known reachable addresses to the remote client.
- To cause the ANG to advertise its known routes, place a check next to Enable Export. This setting is required to allow the ANG to advertise the reachability of virtual subnets to other devices on the network.

7 Do one of the following:

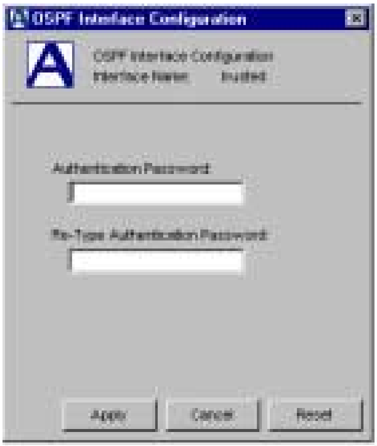
- Click Apply to save the RIP configuration changes.
- Click Cancel to close the window without saving your changes.
- Click Reset to the return the interface’s protocol configuration to its original setting.

Configuring OSPF on an Interface

To enable OSPF on an interface, perform the following steps:

1 Add OSPF as described in “Adding or Removing a Routing Protocol for an Interface” on page 60 or select OSPF from the Routing Protocols list and click Properties.

The OSPF Interface Configuration window appears as shown in Figure 37.



OSPF Interface Configuration
Interface Name Trusted

Authentication Password

Re-Type Authentication Password

Figure 37 Routing Interfaces Configuration - OSPF

2 Type the OSPF password used by routers on your network in the Authentication Password field.

OSPF authentication passwords are used by routers to determine if they should accept updated routing information sent from another router. If your routers do not authenticate updates, leave this field blank.

NOTE

Passwords are limited to 8 characters or less

3 Type the same password in the Re-Type Authentication Password field exactly as you entered it in Step 2.

4 Do one of the following:

- Click Apply to save the OSPF parameter changes.
- Click Cancel to close the window without saving your changes.
- Click Reset to the return the interface's protocol properties to their default settings.

Creating Static Routes

To configure a static route between an ANG interface and another device, perform the following steps:

1 Open the Configuration pullout.

2 In the list of Aurorean devices, expand the tree list under Servers (click the + symbol).

3 Expand the tree list under the name of your ANG.

4 Click on Routing to display the routing parameter tab pages.

5 Click on the Interface tab to display the routing protocol(s) selected for each interface.

6 From the Interfaces menu, choose the ANG Ethernet interface to configure (External or Trusted).

7 In the Routing Protocol Selection list, double click Static Routes and click Add in the Static Route Configuration window.

The Static parameter tab page is displayed as shown in Figure 38.

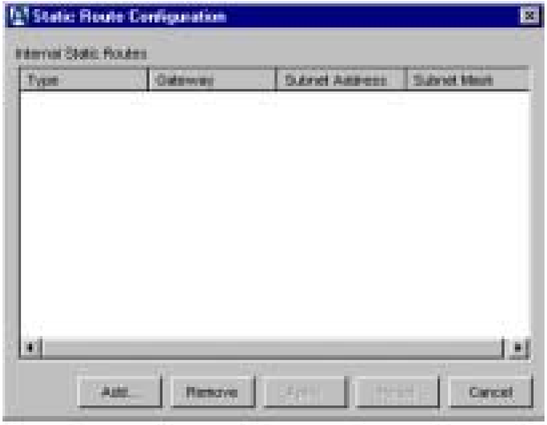


Figure 38 Static Routing Configuration

8 In the Gateway address fields, type the IP address of a gateway on this subnet.

For External interfaces, enter the IP address of the router that provides access to the Internet.

9 In the Reachable Subnet fields, type a starting IP address and subnet mask to define a subnet.

Packets received by the ANG are statically routed to the gateway you specified. To forward all packets to the gateway when there is no other reachable "next hop" address for a packet, enter an address of **0.0.0.0** and a subnet mask of **0.0.0.0**.

CAUTION

Configuring a default static route (0.0.0.0/0.0.0.0) on the *Trusted* interface of the ANG disables Intelligent Client Routing. Refer to "Intelligent Client Routing" on page 31 for more information.

10 Click Add.

The static route you configured appears in the Internal Static Routes display.

11 Do one of the following:

- Click Apply to create the static route.
- Click Reset to the return the interface’s protocol properties to their default settings.
- Click Cancel to close the window without saving your changes.

Adding a Remote Server

An ANG can be added at a remote location in a Site-to-Site configuration. This section describes how to set up an *initiating* Network Gateway to connect to a Local or *terminating* ANG / APS pair.

NOTE

Local ANGs use an accompanying APS; *remote* ANGs are stand-alone.

These instructions *cannot* be used to configure a stand-alone ANG connection to another stand-alone ANG (refer to *Appendix B* for more information).

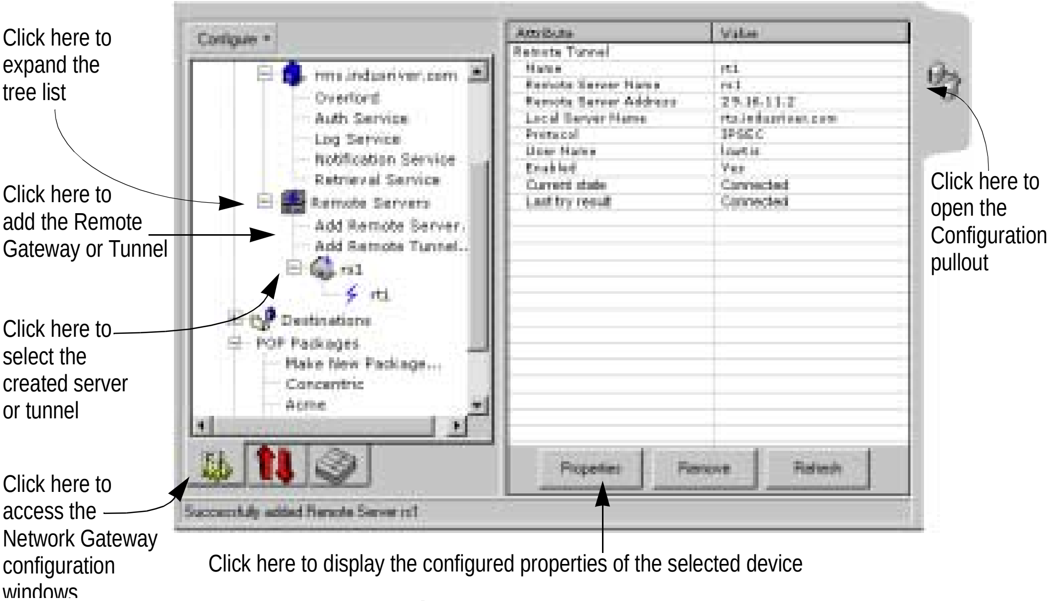
To add a Remote Network Gateway, perform the following steps.

1 Open the Configuration pullout.

2 In the list of Aurorean devices, expand the tree list under gateways (click the + symbol).

3 Expand the tree list under Remote Servers.

The Tunnel Protocols window appears as shown in Figure 39.


Click here to expand the tree list
Click here to add the Remote Gateway or Tunnel
Click here to select the created server or tunnel
Click here to access the Network Gateway configuration windows
Click here to open the Configuration pullout
Click here to display the configured properties of the selected device
Configure ▾
rms.indusriver.com
Overlord
Auth Service
Log Service
Notification Service
Retrieval Service
Remote Servers
Add Remote Server...
Add Remote Tunnel...
rs1
rt1
Destinations
POP Packages
Make New Package...
Concentric
Acme
Properties
Remove
Refresh

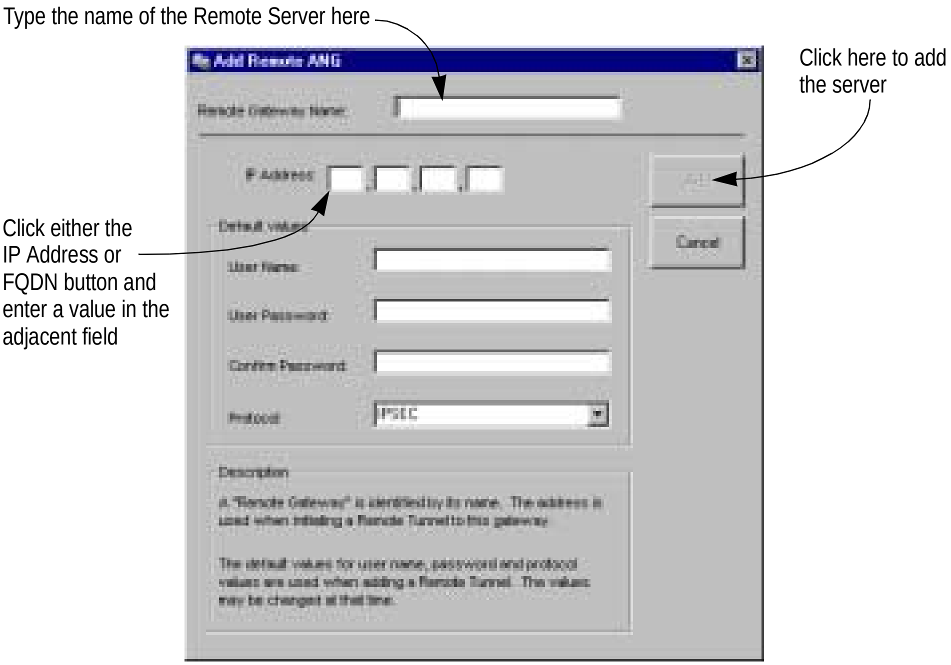
Attribute	Value
Remote Tunnel	
Name	rt1
Remote Server Name	rs1
Remote Server Address	29.18.11.2
Local Server Name	rtc.indusriver.com
Protocol	IPSEC
User Name	louttis
Enabled	Yes
Current state	Connected
Last try result	Connected

Successfully added Remote Server rs1

Figure 39 Remote Server Display

4 Click Add Remote Server.

The Add Remote Server window appears as shown in Figure 40.



A "Remote Gateway" is identified by its name. The address is used when initiating a Remote Tunnel to this gateway.

The default values for user name, password and protocol values are used when adding a Remote Tunnel. The values may be changed at that time.

Type the name of the Remote Server here

Click here to add the server

Click either the IP Address or FQDN button and enter a value in the adjacent field

Figure 40 Add Remote Server Window

5 Choose a name for the server in the Remote Server Name window.

6 Click either IP Address or FQDN (Fully Qualified Domain Name). If you choose IP Address, enter an IP address in the fields provided. If you choose FQDN, enter a value in the single field.

The FQDN is the name of the Remote Server as well as its domain. For example: `server1.argus.com`

7 Type a User Name and User Password and confirm the password in the fields provided.

This User Name and Password must later be registered in the authentication database of the Remote (*terminating*) ANG by adding the user to a group (Refer to Chapter 6 for more information).

8 Choose the tunneling protocol: IPSec or PPTP.

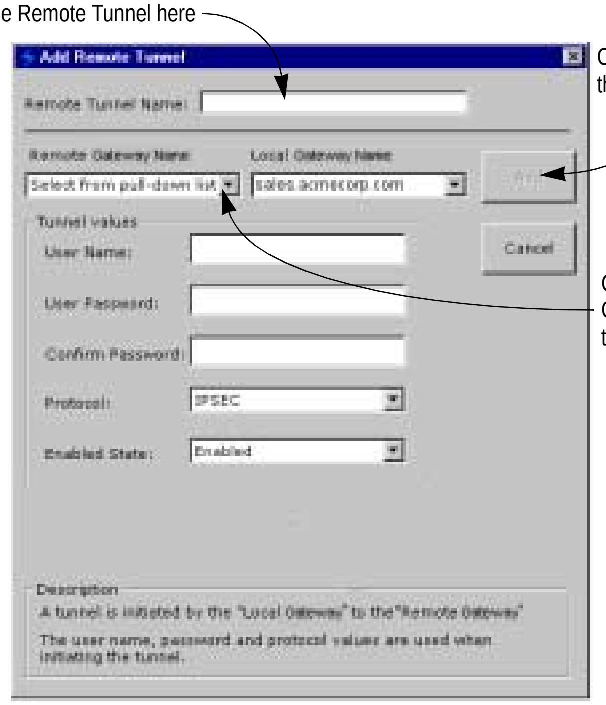
9 Click Add.

This action adds the remote ANG to the configuration on your Local ANG. A message will display stating you have successfully added the remote server.

10 Click Add Remote Tunnel or select the Remote Server just added and click Add Tunnel.

The Add Remote Tunnel window appears as shown in Figure 41.

Type the name of the Remote Tunnel here



Add Remote Tunnel

Remote Tunnel Name:

Remote Gateway Name: Select from pull-down list

Local Gateway Name: sales.acmecorp.com

Tunnel values

User Name:

User Password:

Confirm Password:

Protocol: IPSEC

Enabled State: Enabled

Description

A tunnel is initiated by the "Local Gateway" to the "Remote Gateway"

The user name, password and protocol values are used when initiating the tunnel.

Click here to add the tunnel

Choose the Remote Gateway name from this pull-down list

Figure 41 Add Remote Tunnel Window

11 Choose a name for the Remote Tunnel in the provided field.

12 Click the arrow in the Remote Server Name field to bring up a pull-down list and select the Remote Server you just added.

RiverMaster types the Server user name and password into the open fields. You may change these settings if necessary.

13 Select Enabled or Disabled in the Enabled State field.

If you select Enabled, the tunnel will be created immediately. Select Disabled if you want to delay enabling the tunnel until configuration is complete at the other end of the tunnel.

14 Click Add.

If the Enabled state was selected earlier, the tunnel becomes operational in a few moments.

NOTE

You can configure additional tunnels to the Remote Server just added by selecting the particular server in the Remote Tunnels display, clicking Properties, and clicking Add Tunnel in the Remote Server Properties window.

Changing Server and Tunnel Properties

The information configured for Site-to-Site servers and tunnels can be changed by clicking the Properties buttons on either display.

To change properties for the Remote Server, perform the following steps:

1 Select your Remote Server from the tree list under Remote Servers and click Properties in the display.

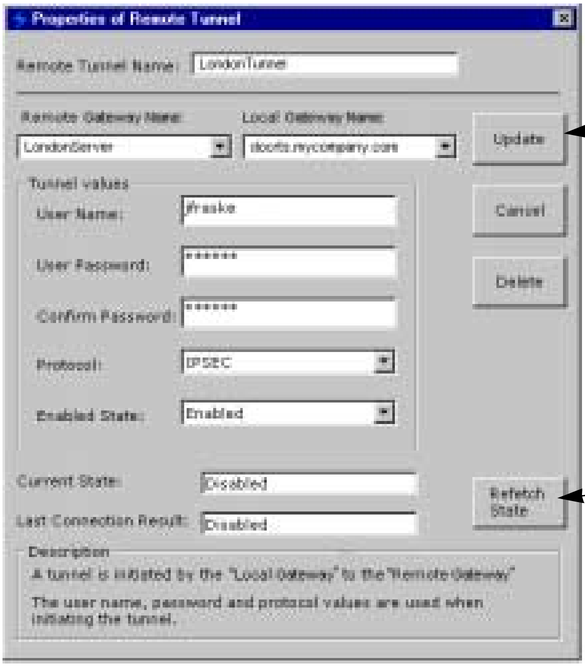
2 When the Remote Server Properties window appears, change any information and do one of the following:

- Click Modify to reconfigure the Remote Server.
- Click Cancel to close the window without saving your changes.
- Click Delete to remove the Remote Server configuration.

To change properties for the Remote Tunnel, perform the following steps:

1. Select your Remote Tunnel from the tree list under Remote Servers and click Properties in the display.

   The Remote Tunnel Properties window appears as shown in Figure 42.



Remote Tunnel Name: LondonTunnel

Remote Gateway Name: LondonServer

Local Gateway Name: docfs.mycompany.com

Tunnel values

User Name: jfraske

User Password: ******

Confirm Password: ******

Protocol: IPSEC

Enabled State: Enabled

Current State: Disabled

Last Connection Result: Disabled

Description

A tunnel is initiated by the "Local Gateway" to the "Remote Gateway"

The user name, password and protocol values are used when initiating the tunnel.

Click here to update the tunnel

Click here to refresh the values for the Current state and Last try result attributes shown in the Tunnel Protocols window

Figure 42 Remote Tunnel Properties Window

2. Change any information. If the Remote Tunnel is enabled, select Disabled in the Enabled State field and do one of the following:

   – Click Update to reconfigure the Remote Tunnel.
   – Click Cancel to close the window without saving your changes.
   – Click Delete to remove the Remote Tunnel configuration.

   If you clicked Update, a window pops up asking if you want to save the modified tunnel. Click Yes or No.

3 Re-open the Remote Tunnel Properties window and select Enabled in the Enabled State field if you want to create the tunnel immediately with the reconfigured properties.

If you clicked Update, a window pops up again asking if you want to save the modified tunnel. Click Yes or No.

NOTE

Clicking Refresh displays the status for the Current State and Last Connection Result attributes of the tunnel.

4

Setting Up Aurorean Services

This chapter describes how to perform the following tasks:

- ❐ Add an Authorization service plug-in to allow Aurorean Virtual Network systems to authenticate remote users against a local database on the Aurorean Policy Server, an external Remote Authentication Dial In User Service (RADIUS) server, or an RSA ACE / Server.
- ❐ Generate private / public encryption / decryption keys for use with the IPSec protocol.
- ❐ Prepare the Notification server on the APS to send E-mail when alarm, alert, or notification messages are generated.
- ❐ Adjust trace levels for Management and Tunnel server services to generate a controlled stream of messages.
- ❐ Backup the Management Database to avoid operational down time.

Before You Begin

Before performing the steps in this chapter, you should familiarize yourself with the following Aurorean Virtual Network concepts:

- ❐ Authorization plug-in options
- ❐ Private / public keys for IPSec authentication
- ❐ Problem notification via E-mail
- ❐ Trace levels

Authorization Plug-in Options

Within a Aurorean Virtual Network, the APS coordinates remote user authentication. Using an internal software service known as Authentication and a series of “plug-ins”, the APS can authenticate remote users in three ways:

- ❒ Using the Enterasys Authentication plug-in, remote users are authenticated against a database residing on the APS’s hard drive.
- ❒ Using the RADIUS plug-in, the APS acts as a RADIUS client, forwarding authentication requests from Aurorean users to a RADIUS server.
- ❒ Using the RSA Security SecurID plug-in, the APS acts as a native ACE/Client, forwarding authentication requests from Aurorean users directly to an ACE/Server. This plug-in supports the fail-over function of automatically connecting to a slave ACE/Server if the master fails.

RADIUS Authentication Servers

Aurorean Virtual Network systems support a wide range of RADIUS servers, including:

- ❒ Microsoft RADIUS
- ❒ Funk Software’s Steel-Belted RADIUS
- ❒ RSA Security ACE/Server that supports RADIUS extensions. This allows remote users to not only authenticate against a centralized authentication database, but also to take advantage of the strong security offered by SecurID passcodes.
- ❒ Novell’s BorderManager™ Authentication Services (BMAS) running on a RADIUS server. BMAS is an interface that links dial-in users to the network through Novell Directory Services (NDS™). Support for BorderManager is seamless and it requires no configuration on the APS. Refer to BorderManager Enterprise Edition documentation for more information.

NOTE

Enterasys Networks continually tests interoperability with other RADIUS server vendors. Contact Enterasys Networks Customer Support for an up-to-date list of approved RADIUS servers.

Plug-in Planning

You can add multiple plug-ins for RADIUS or SecurID authentication. Typically, you add one plug-in for each RADIUS or SecurID authentication server on your network and preserve the Enterasys Authentication plug-in for RiverMaster logins. One plug-in must be designated as the default plug-in. When you set up your Aurorean Virtual Network for the first time, the default plug-in is Enterasys Authentication.

When Aurorean users attempt to tunnel into the corporate network, they must present a VPN user name and password for authentication. If the Aurorean Client user presents a simple user name such as **BSmith**, the user is authenticated against the default plug-in. Aurorean users have the ability to override the default and select another plug-in by adding an “@” symbol and the identifier for the plug-in. For example, if you add a RADIUS plug-in with the identifier **RADIUS1**, a Aurorean Client user can select this plug-in by entering a VPN user name such as **BSmith@RADIUS1**.

Threads

You can accelerate the authentication of multiple users logging in at the same time by increasing the number of threads (logins in progress) the authenticating server will handle. This function is useful if you discover that users are exceeding the timeout value allowed for authentication and are not being connected because too many clients are dialing in simultaneously.

For instructions on customizing the Enterasys Authentication plug-in and adding RADIUS and SecurID plug-ins, refer to “Adding an Authorization Plug-In” on page 80.

Private/Public Keys for IPSec Authentication

Aurorean users who tunnel into your network using the IPSec protocol also require an El Gamal *public key* for authentication. The key is an embedded piece of data used to encrypt and decrypt packets exchanged between Aurorean Client and the Aurorean Network Gateway. A pair of keys, one private and one public, are generated and saved on the APS.

The public key is included in the Aurorean Client installation kit you build and distribute for your remote users (as described in Chapter 6). The exchange of keys is handled entirely by the Aurorean Client application; the user does not need to know or type the public key.

However, if the private key on the APS becomes compromised, you may need to regenerate the private / public key pair and distribute files with the new public key to your remote users. Without the current public key, IPSec users will be unable to tunnel into the network. For instructions on generating a new private / public key pair, refer to “Generating Private / Public Keys” on page 91.

Problem Notification

The Notification service that runs on both the Management and Tunnel servers generate messages when the server experiences operational difficulty. The events that trigger these messages fall into three categories:

- ❒ *Alarms* notify you when a significant error occurs with a service running on a Aurorean Virtual Network system or a general system problem that is preventing the server from operating normally.
- ❒ *Alerts* occur when an error count threshold has been crossed and an alarm condition is imminent.
- ❒ A *Problem Notification* typically indicates a remote client connection problem which Aurorean Client’s Prescriber feature diagnosed.

These messages appear in the View System Activity pullout and advanced message viewer (as described in Chapter 7) and can also be retrieved from system reports (as described in Chapter 8). For immediate notification when one of these events occurs, the APS can send E-mail to one or more persons that you select. You must first define a mailing list and then add E-mail addresses for each recipient to this list. You can select which types of messages (alarms, alerts, or problem notifications) will be sent to each address.

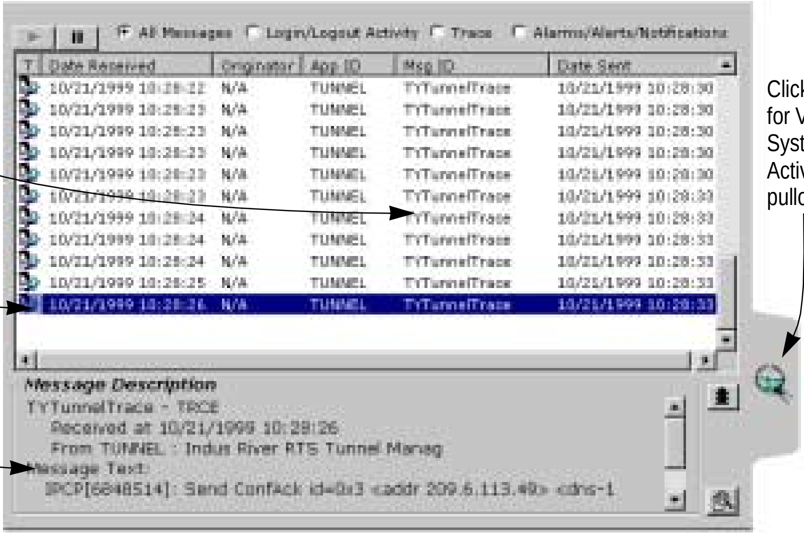
For instructions on creating mailing lists for problem notification, refer to “Using the Notification Service to Send E-Mail” on page 93.

Trace Levels

The number of messages the Management and Tunnel servers report to RiverMaster can be set on a per service basis. Because so many messages are routinely shared via control traffic between the servers and clients, if a limit were not set on their collection and display they could disrupt Aurorean Virtual Network service. But, having the option to occasionally read these messages can help troubleshoot service problems. Refer to Chapter 7 for more detailed information on the types of messages displayed.

RiverMaster permits you to set *low*, *medium* or *high* trace levels for the ten available Enterasys services. These levels correspond to varying numbers of messages reported to RiverMaster, depending on the service you configure.

For example, a *low* trace level set for the Tunnel Management Service will produce messages similar to those in Figure 43.



T	Date Received	Originator	App ID	Msg ID	Date Sent
	10/21/1999 10:28:22	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:30
	10/21/1999 10:28:23	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:30
	10/21/1999 10:28:23	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:30
	10/21/1999 10:28:23	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:30
	10/21/1999 10:28:23	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:30
	10/21/1999 10:28:23	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:33
	10/21/1999 10:28:24	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:33
	10/21/1999 10:28:24	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:33
	10/21/1999 10:28:24	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:33
	10/21/1999 10:28:25	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:33
	10/21/1999 10:28:26	N/A	TUNNEL	TYTunnelTrace	10/21/1999 10:28:33

Message Description

```
TYTunnelTrace - TRCE
   Received at 10/21/1999 10:28:26
   From TUNNEL : Indus River RTS Tunnel Manag
Message Text:
  IPCP[6848514]: Send ConfAck id=0x3 <addr 209.6.113.49> <dns-1
```

Note Tunnel Trace messages sent by the tunnel server

Highlighted message here is detailed in description area below

See message text here

Click here for View System Activity pullout

Figure 43 Trace Messages Display

If you read the text for each Tunnel Trace message above, you can follow the chain of protocol messages which signify the communications that occur on a packet level when a client successfully makes a connection. Then, if a client connection subsequently fails, you could compare messages and troubleshoot the problem. For instructions on setting trace levels, refer to “Setting Trace Levels” on page 97.

Adding an Authorization Plug-In

The Enterasys Authentication plug-in is factory-installed by Enterasys Networks and made the default plug-in. This plug-in is used when you log into the RiverMaster application to ensure that you have administration privileges. To support SecurID and RADIUS authentication, you must add one or more SecurID or RADIUS plug-ins.

NOTE

Do not remove the Enterasys Authentication plug-in or convert it into a RADIUS or SecurID plug-in. Without a plug-in of this type, you will not be able to log into RiverMaster.

Enterasys Authentication

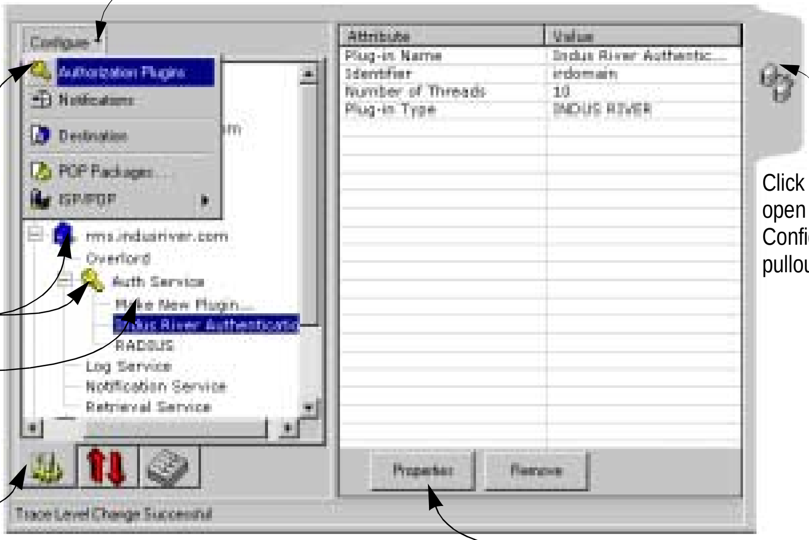
To modify the Enterasys Authentication plug-in, perform the following steps:

1 Open the Configuration pullout.

2 In the list of Aurorean devices, expand the tree list (by clicking the + symbol) under the name of your APS, and expand it again under Auth Service.

Figure 44 shows the Configuration pullout.

Click here to view Configure pull-down box options



Attribute	Value
Plug-in Name	Indus River Authentic...
Identifier	irdomain
Number of Threads	10
Plug-in Type	INDUS RIVER

Trace Level Change Successful

Click here to add a new Authorization Plug-in or here to expand the tree list and select or create a plug-in

Click here to access the APS configuration windows

Click here to open the Configuration pullout

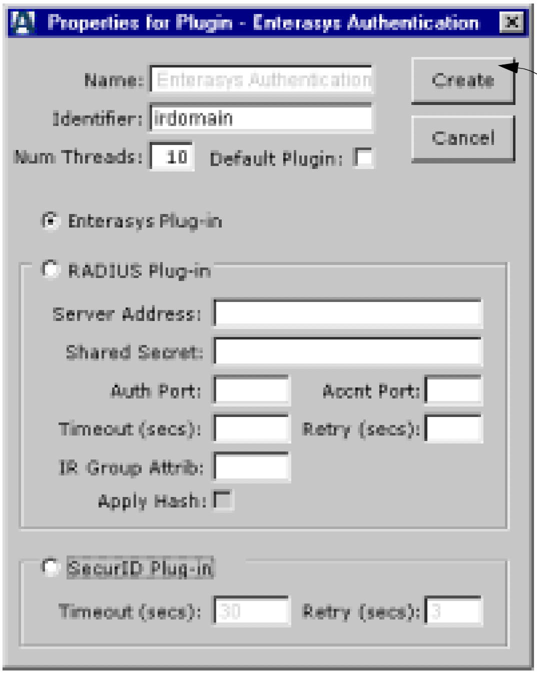
Click here to configure the plug-in

Figure 44 Configure Authorization Plug-ins Window

3 From the list of Plug-ins, select Enterasys Authentication.

4 Click Properties.

The Properties for Plug-in - Enterasys Authentication window will appear as shown in Figure 45.



Properties for Plugin - Enterasys Authentication

Name: Enterasys Authentication
Identifier: irdomain
Num Threads: 10
Default Plugin: ☐

● Enterasys Plug-in

○ RADIUS Plug-in
Server Address:
Shared Secret:
Auth Port:
Accnt Port:
Timeout (secs):
Retry (secs):
IR Group Attrib:
Apply Hash: ☐

○ SecurID Plug-in
Timeout (secs): 30
Retry (secs): 3

Click here to update the plug-in

Figure 45 Enterasys Authentication Plug-in Window

5 In the Identifier field, type a name that remote users will use to select this plug-in.

Aurorean users can include this identifier as part of their VPN user names to override the default authorization plug-in. For example, if you enter **Enterasys** as the identifier for this plug-in, Aurorean users can specify a user name such as **Bob@Enterasys** to ensure that they authenticate against the APS.

6 Optionally, specify a value in the Num Threads field.

This function allows the specified number of users to simultaneously log in without delay. The range of threads that can be set is 1 to 100, with a default value set to 10.

7 If you want to make this plug-in the default authorization method, check the Default Plug-In box.

8 Do one of the following:

- Click Update to save your changes.
- Click Cancel to clear the fields without saving the plug-in.

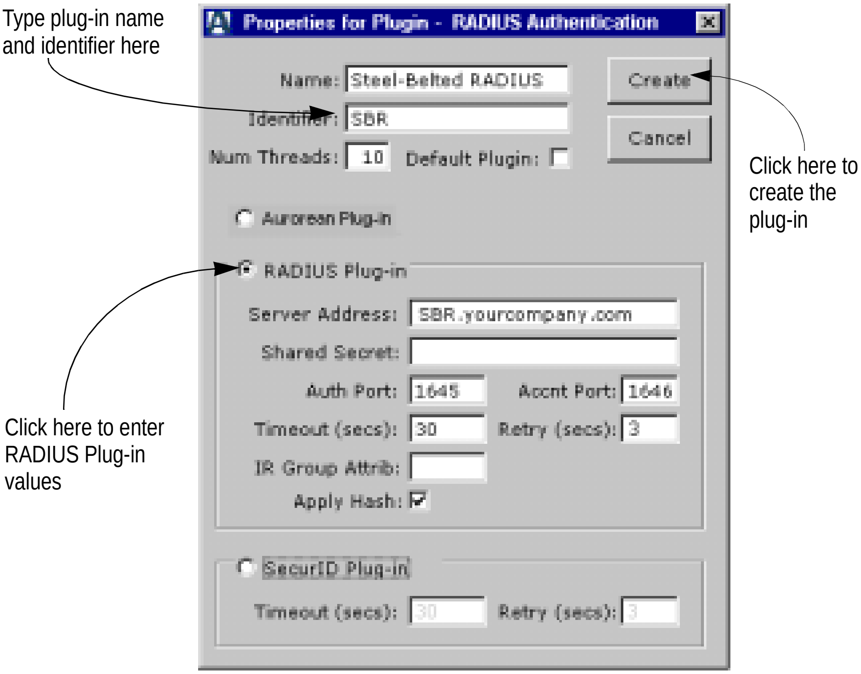
RADIUS Authorization

To configure the APS to forward authentication requests to a RADIUS server, perform the following steps:

1 Open the Configuration pullout.

2 Choose Authorization Plug-ins from the Configure pull-down box in the top left corner of the pullout. Or, in the list of Aurorean Virtual Network devices, expand the tree list under the name of your APS (by clicking the + symbol), expand it again under Auth Service and click Make New Plug-in...

The Create New Plug-in window will appear as shown in Figure 46, but without default or configured values.



Properties for Plugin - RADIUS Authentication

Name: Steel-Belted RADIUS
Identifier: SBR
Num Threads: 10 Default Plugin: □

○ Aurorean Plug-in

● RADIUS Plug-in

Server Address: SBR.yourcompany.com
Shared Secret:
Auth Port: 1645 Accnt Port: 1646
Timeout (secs): 30 Retry (secs): 3
IR Group Attrib:
Apply Hash: ☑

○ SecurID Plug-in

Timeout (secs): 30 Retry (secs): 3

Type plug-in name and identifier here

Click here to create the plug-in

Click here to enter RADIUS Plug-in values

Figure 46 Sample RADIUS Authorization Plug-In Settings

3 In the Name field, type in a name to describe the plug-in.

This name later appears in the plug-in tree list. For example, if you are adding a plug-in for a Steel-Belted RADIUS server, you can type **Steel-Belted RADIUS** as the name. If you plan to authenticate against more than one RADIUS server, you can enter a specific server name in this field.

4 In the Identifier field, type a name that remote users will use to select this plug-in.

Aurorean users can include this identifier as part of their VPN user names to override the default authorization plug-in. For example, if you enter **RADIUS** as the identifier for this plug-in, Aurorean users can specify a user name such as **Bob@RADIUS** to authenticate against the RADIUS server instead of the default plug-in.

5 Optionally, specify a value in the Num Threads field.

This function allows the specified number of users to simultaneously log in without delay. The range of threads that can be set is 1 to 100, with a default value set to 10.

✓ NOTE

Do not set Num Threads to a 0 (zero) value for a RADIUS plug-in. This will cause user login problems. You may set the value to zero for the Enterasys Authentication plug-in.

6 To make this plug-in the default authorization method, place a check next to Default Plug-In.

7 Click on Radius Plug-In.

8 In the Server Address field, enter the IP address or DNS name of the RADIUS server.

9 In the Shared Secret field, type the same shared secret password you entered on the RADIUS server.

For more information on shared secrets, refer to the documentation supplied with your RADIUS server.

10 Leave the Authentication Port and Accounting Port fields set to their default values.

These values specify UDP port numbers and match industry standards for RADIUS.

11 In the Timeout field, enter the number of seconds the APS should wait before resending an authentication request.

If the RADIUS server fails to respond to an authentication request within the time specified, the APS automatically resends the request. Depending upon the type of RADIUS server you use, set this field as follows:

Server Type	**Recommended Value**
Steel-Belted RADIUS	10 seconds
MS RADIUS	10 seconds
SecurID over RADIUS	30 seconds

12 In the Retry field, enter the number of times the APS should resend an authentication request.

For example, when this field is set to 2, the APS resends an authentication request twice before declaring the RADIUS server unreachable. Depending upon the type of RADIUS server you use, set this field as follows:

Server Type	**Recommended Value**
Steel-Belted RADIUS	3 retries
MS RADIUS	3 retries
SecurID over RADIUS	1 retry

13 If you were unable to create an Enterasys group on your RADIUS server and need to reuse an existing group attribute, enter the attribute number in the Group Attrib. field.

Authentication messages passed between the APS and the RADIUS server must carry a group attribute. If the RADIUS server management application prevented you from creating an Enterasys group attribute, you can take over a pre-defined attribute and use it for VPN authentication. For example, the standard attribute Login-LAT-Group can be used by entering its number, **36**, in this field. For a complete list of attribute numbers, refer to the IETF RFC 2138.

14. If you want the APS to apply an MD4 hash to the key returned by the RADIUS server, place a check next to the Apply Hash field.

    Place a check in this field only if all of the following statements are *true*: remote users will authenticate against a Steel-Belted RADIUS 2.1 or earlier server, the tunnel protocol negotiated for all connections by these users will be PPTP, and 128-bit encryption is enabled on the Aurorean Network Gateway.

15. Do one of the following:
    – Click Commit to save the new plug-in.
    – Click Cancel to clear the fields without saving the plug-in.

16. If you click Commit, you are prompted to re-type the Shared Secret.

17. Reboot the APS to enable the authorization changes.

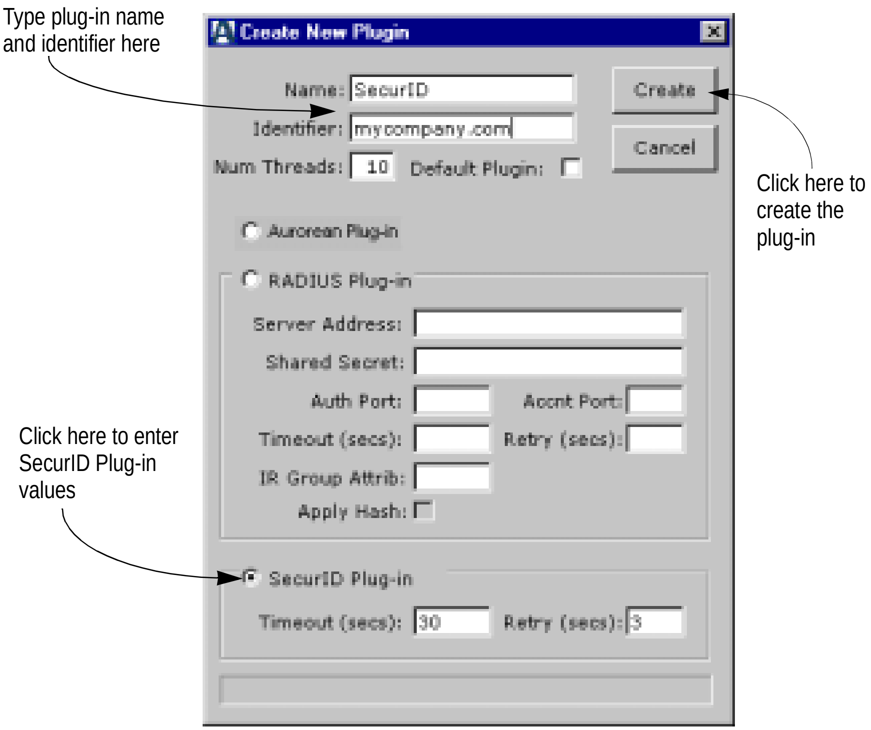
SecurID Authorization

To configure the APS to forward authentication requests to a SecurID server, perform the following steps:

1. Open the Configuration pullout.

2. Choose Authorization Plug-ins from the Configure pull-down box in the top left corner of the pullout. Or, in the list of Aurorean devices, expand the tree list under the name of your APS (by clicking the + symbol), expand it again under Auth Service and click Make New Plug-in ...

   The Create New Plug-in window will appear as shown in Figure 47.



Name: SecurID
Identifier: mycompany.com
Num Threads: 10
Default Plugin: □

○ Aurorean Plug-in

○ RADIUS Plug-in

● SecurID Plug-in
Timeout (secs): 30
Retry (secs): 3

Type plug-in name and identifier here

Click here to create the plug-in

Click here to enter SecurID Plug-in values

Figure 47 SecurID Plug-in Window

3 In the Name field, type in a name to describe the plug-in.

This name later appears in the plug-in tree list. For example, if you are adding a plug-in for a SecurID server, you can type **SecurID** as the name. If you plan to authenticate against more than one SecurID server, you can enter a specific server name in this field.

4 In the Identifier field, type a name that remote users will use to select this plug-in.

Aurorean users can include this identifier as part of their VPN user names to override the default authorization plug-in. For example, if you enter **ACE** as the identifier for this plug-in, Aurorean users can specify a user name such as **Bob@ACE** to authenticate against the ACE/Server instead of the default plug-in.

5 Optionally, specify a value in the Num Threads field.

This function allows the specified number of users to simultaneously log in without delay. The range of threads that can be set is 1 to 100, with a default value set to 10.

6 To make this plug-in the default authorization method, place a check next to Default Plug-In.

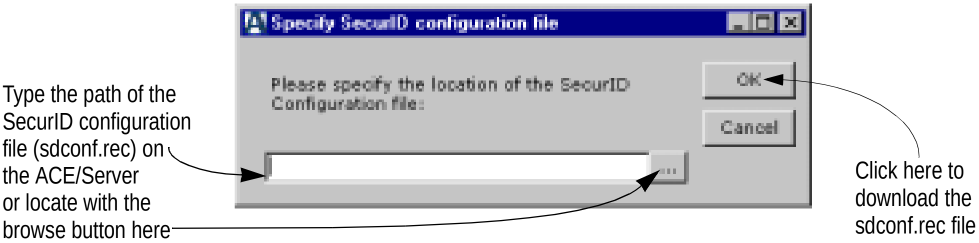
7 Click on SecurID Plug-in.

8 Optionally, you can change the values for Timeout and Retry from the default values displayed.

Timeout is the interval in seconds before another authorization attempt is made by the APS. Retry is the number of authorization attempts you will permit the APS to try.

9 Click Create.

The Specify SecurID configuration file window appears as shown in Figure 48.



Specify SecurID configuration file

Please specify the location of the SecurID Configuration file:

OK
Cancel
...
Type the path of the SecurID configuration file (sdconf.rec) on the ACE/Server or locate with the browse button here
Click here to download the sdconf.rec file

Figure 48 Specify SecurID Configuration File Window

10 Type the path of the SecurID configuration file (`SDCONF.rec`) in the ACE/Server and click OK or find the file on the network by clicking the browse button to the right of the field.

If you typed the correct path of the configuration file, it is downloaded to its proper site on the APS and the plug-in saved. If you clicked the browse button, an Open window appears prompting you to locate the file. When you find and select it, click Open and the Specify SecurID configuration file window will reappear. Then click OK and the process is complete. Optionally, you can copy the file off the ACE/Server to a floppy disk, load the disk in the RiverMaster floppy drive, and browse for the file on the `a:` drive.

✓ NOTE

If a new `SDCONF.rec` becomes available, select the SecurID plug-in from the Auth Service list, click Properties and Update Configuration File, and repeat Step 10.

Generating Private/Public Keys

A unique El Gamal private / public key pair is produced on all APSs. In most cases, these keys do not need to change. However, if you believe the keys have been compromised and your network security is subject to risk, you can generate a new El Gamal private / public key pair by performing the following steps:

NOTE

When you regenerate the El Gamal private / public keys, Aurorean users who employ IPSec protocol cannot tunnel into the corporate network until a set of core files containing the new public key are distributed. To build core files that contain the new key, refer to the instructions in Chapter 6.

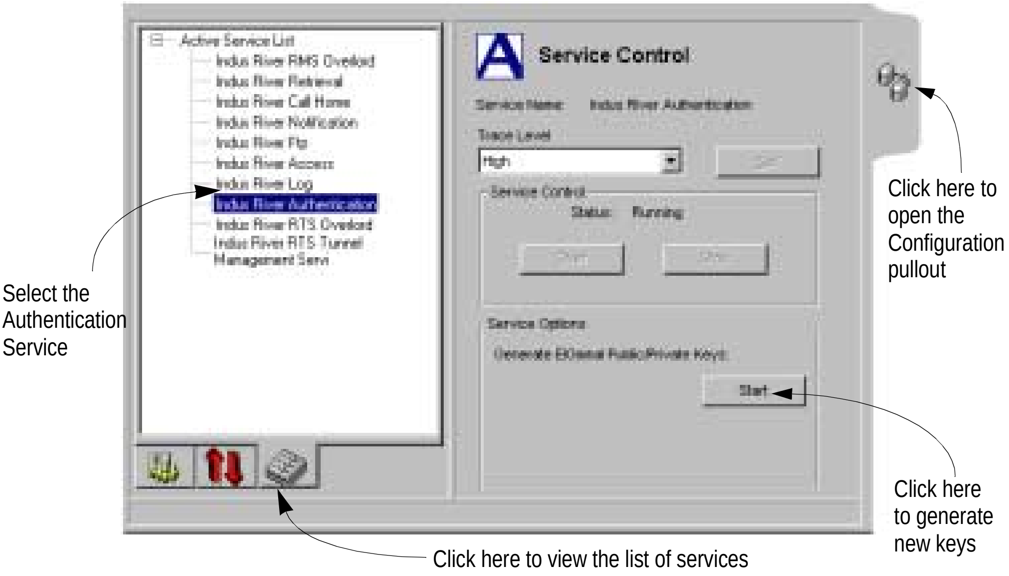
1 Open the Configuration pullout.

2 Click on the Activity icon in the lower left corner of the pullout to switch to the Active Tunnel/Service List view.

3 Expand the tree list under Active Service List (click the + symbol).

4 Click on Enterasys Authentication.

The Service Control display for the Authentication Service appears as shown in Figure 49.



Active Service List
- Indus River RMS Overload
- Indus River Retrieval
- Indus River Call Home
- Indus River Notification
- Indus River Ftp
- Indus River Access
- Indus River Log
- Indus River Authentication
- Indus River RTS Overload
- Indus River RTS Tunnel Management Servi

Service Control

Service Name: Indus River Authentication

Trace Level: High

Service Control
Status: Running

Service Options
Generate ElGamal Public/Private Keys:

Select the Authentication Service

Click here to open the Configuration pullout

Click here to generate new keys

Click here to view the list of services

Figure 49 Generating El Gamal Private/Public Keys

5 Click Start to begin generating a new private/public key pair.

NOTE

This display can also be used to start and stop the Authentication Service. Because terminating this service can prevent remote clients from connecting to the Aurorean Network Gateway, stopping this service should be done only when recommended by Enterasys Networks Customer Support personnel.

Using the Notification Service to Send E-Mail

There are two stages to setting up the Notification service:

- ❒ Creating a mailing list
- ❒ Adding addresses to a list

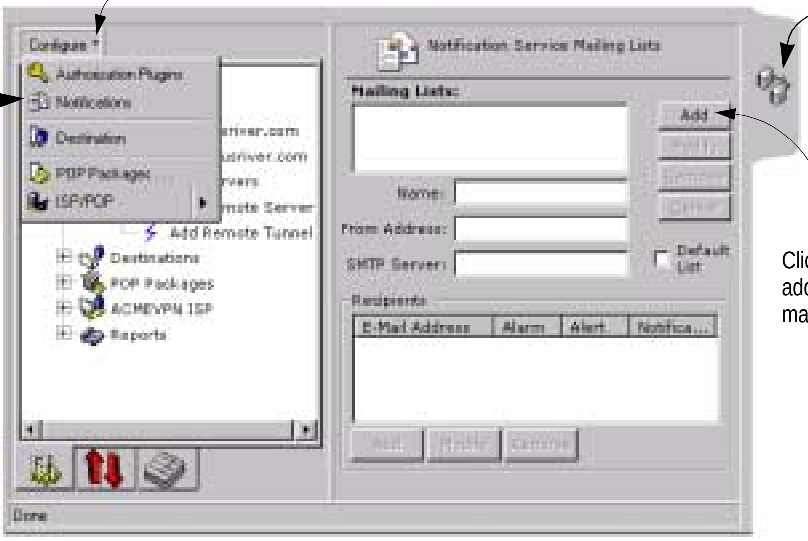
Creating a Mailing List

The RiverMaster installation process creates an initial mailing list called DEFAULT. To create your own custom mailing list, perform the following steps:

1 Open the Configuration pullout.

2 Choose Notifications from the Configure pull-down box in the top left corner of the pullout.

Figure 50 shows the Configuration pullout with the Notification Service Mailing Lists display selected.



Click here to view Configure pull-down box options

Click here to open the Configuration pullout

Click here to select Notifications

Click here to add a new mailing list

Figure 50 Notification Service Mailing List Window

3 Click Add (the Add button to the right of Mailing Lists).

4 In the Name field, type a descriptive name for this mailing list.

5 In the From Address field, enter the E-mail address that will appear as the originator for E-mails sent to members of this list.

Instead of using your E-mail address or the address of another person, you can create a new address for the APS, such as **Aurorean@Acme.com**.

6 In the SMTP Server field, enter the name of the SMTP server on your network.

Simple Mail Transfer Protocol (SMTP) servers typically follow the naming convention SMTP.*Company*.com where *Company* is the company name used throughout your network.

7 To make the new list the default mailing list, place a check next to Default List.

8 Do one of the following:

- Click Commit to save the new mailing list.
- Click Cancel to clear the mailing list information without saving your changes.

✓ NOTE

When you modify Notification service settings, you must restart the APS to put the changes into effect.

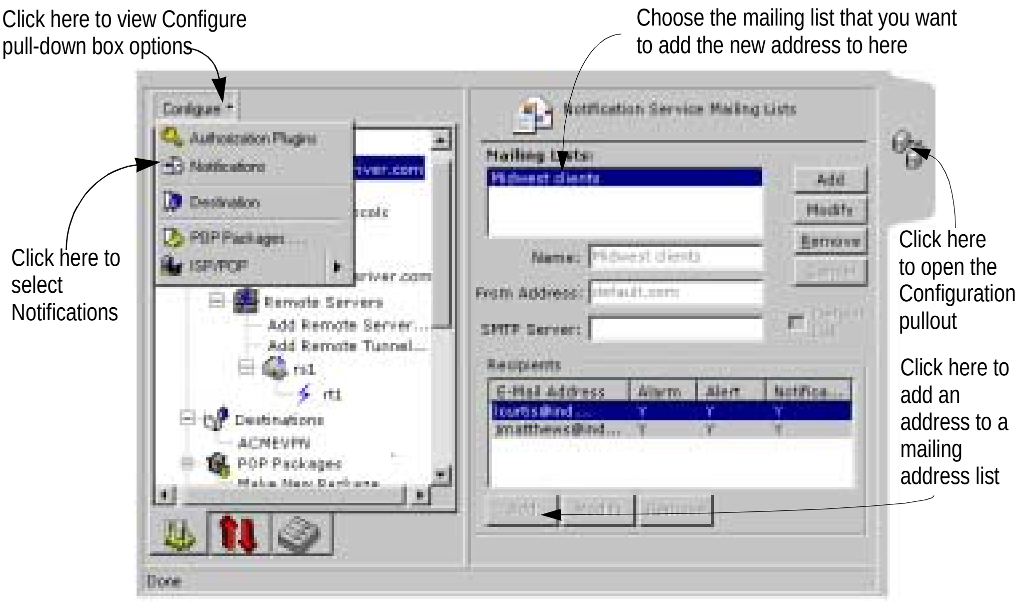
Adding an Address to a Mailing List

To add E-mail addresses to a mailing list, perform the following steps:

1. Open the Configuration pullout.

2. Choose Notifications from the Configure pull-down box in the top left corner of the pullout.

   Figure 51 shows the Configuration pullout with the Notification display selected



Name: Midwest clients

From Address: default.com

E-Mail Address	Alarm	Alert	Notifica...
lcurtis@nd...	Y	Y	Y
jmatthews@nd...	Y	Y	Y

Click here to view Configure pull-down box options

Choose the mailing list that you want to add the new address to here

Click here to select Notifications

Click here to open the Configuration pullout

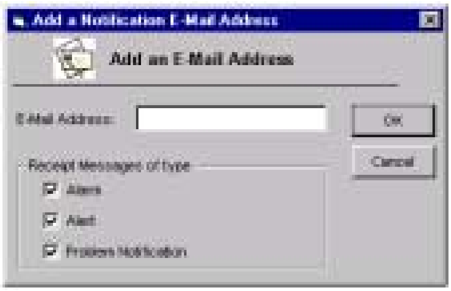
Click here to add an address to a mailing address list

Figure 51 Detailed Notification Service Mailing List Window

3. Select a mailing list from those shown in the Mailing Lists list box and click Modify (the Modify button to the right of Mailing Lists).

4. Click Add (the Add button below the Recipients list).

   An Add a Notification E-Mail Address window appears similar to the one shown in Figure 52.



☑ Alarm
☑ Alert
☑ Problem Notification

Figure 52 Add a Notification E-Mail Address Window

5 In the E-Mail Address field, type the E-mail address of the person you want to receive notification messages.

6 Use the check boxes to select the events which will generate E-mail and click OK.

You can select from the following events:

– *Alarms* notify you when a significant error occurs with a service running on a Aurorean Virtual Network system or a general system problem that is preventing the system from operating normally.

– *Alerts* occur when an error count threshold has been crossed and an alarm condition is imminent.

– A *Problem Notification* typically indicates a remote client connection problem which Aurorean Client’s Prescriber feature diagnosed.

7 Do one of the following:

– Click Update to save the new address to the mailing list.

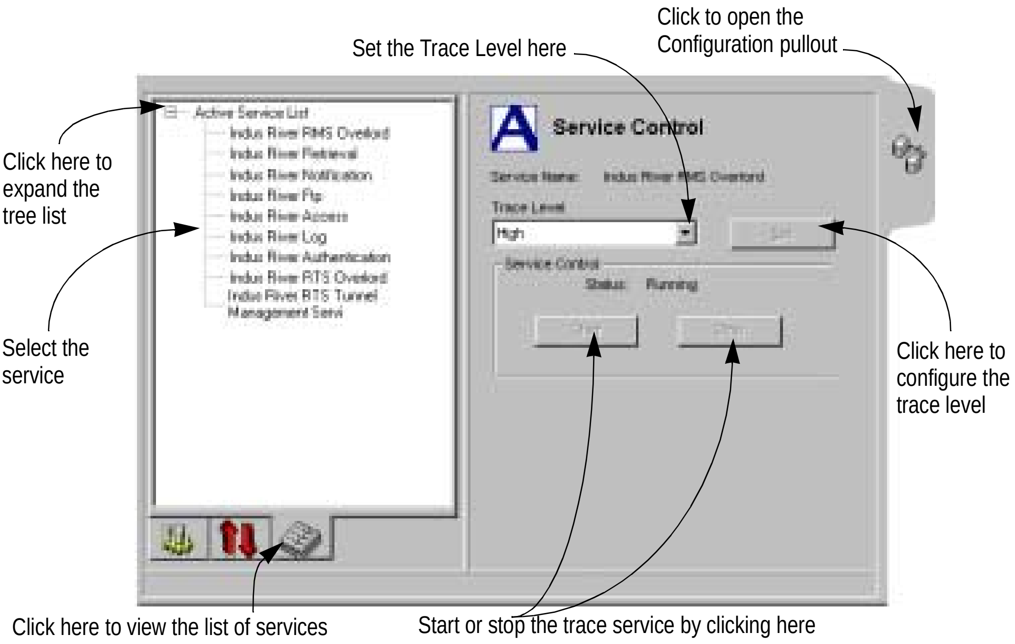
– Click Cancel to clear the mailing list information without saving your changes.

Setting Trace Levels

To set the trace level for any of the ten services, perform the following steps:

1. Open the Configuration pullout.
2. Click on the Activity icon in the lower left corner of the pullout to view the Active Service List.

   Figure 53 shows the Tunnel Management Service window with the full Active Service List displayed.
3. Expand the tree list under Active Service List (click the + symbol).
4. Select the service of your choice.



Active Service List
- Indus River RMS Overlord
- Indus River Retrieval
- Indus River Notification
- Indus River Ftp
- Indus River Access
- Indus River Log
- Indus River Authentication
- Indus River RTS Overlord
- Indus River RTS Tunnel Management Servi

Service Control

Service Name: Indus River RMS Overlord

Trace Level: High

Service Control

Status: Running

Set the Trace Level here

Click to open the Configuration pullout

Click here to expand the tree list

Select the service

Click here to configure the trace level

Click here to view the list of services

Start or stop the trace service by clicking here

Figure 53 ANG Tunnel Management Service Window

5. Click the arrow in the Trace Level field and select None, Low, Medium or High.

   Medium and High trace levels are recommended only for diagnostic purposes and with the supervision of Enterasys Customer Support personnel.

6. Click Set to enable the Trace Level.

RiverMaster now begins tracing messages at the level you set.

NOTE

If you want to *terminate* a particular running service, click Stop. To start up a terminated service, click Start.

Backing Up the Database

The Management database (`management.db`) is a 1Mb file residing on the APS which contains a list of selected ISPs as well as configuration data for both the tunnel and management servers. To avoid the possibility of down time should the database become corrupted, it is advisable to back it up. Consult Enterasys Customer Support for directions to reinstall the database.

Two options are available for saving the database. You can simply copy the file into a default directory on the APS or copy it a second time into a directory of your choice on your management device, a remote network site or to a ZIP device.

To back up the Management database on the APS, perform the following steps:

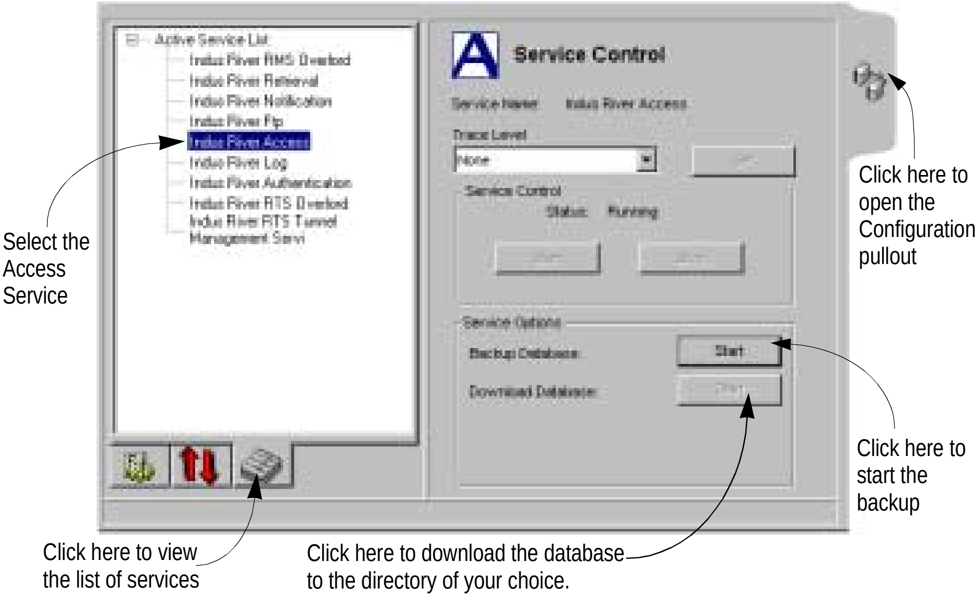
1. Open the Configuration pullout.

2. Click on the Activity icon in the lower left corner of the pullout to switch to the Active Tunnel/Service List view.

3. Expand the tree list under Active Service List (click the + symbol).

4 Click on Indus River Access.

The Service Control display for the Access Service appears as shown in Figure 54.



Select the Access Service

Click here to open the Configuration pullout

Click here to start the backup

Click here to view the list of services

Click here to download the database to the directory of your choice.

Figure 54 Starting a Database Backup

5 Click Start on Backup Database.

A window pops up stating the database and the `.authloc` files were copied to the `C:\IndusRiver\Database\Backup` directory. Click OK. `Authloc` contains a copy of the El Gamal key.

CAUTION

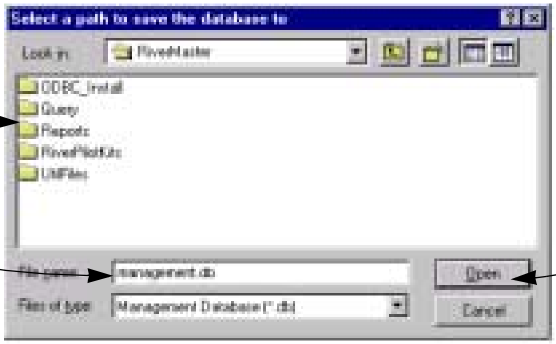
This display can also be used to start and stop the Access Service. Because stopping this service can prevent remote clients from connecting the Aurorean Network Gateway, stopping this service should only be done when recommended by Enterasys Networks Customer Support.

6 Click Start for Download Database to copy the database to a directory of your choice on your computer or a system on the network.

A window similar to Figure 55 will appear.

Select the directory on RiverMaster in which to copy your database

Optionally, type a new name for the database here



Look in: RiverMaster

File name: management.db

Files of type: Management Database (*.db)

Click here to save the database

Figure 55 Select a Path to Save the Database to

7 Keep the default name or retype the database File name, select the directory, and click Open.

RiverMaster copies the database file to the directory of your choice.

For instructions on using this file to restore your management database, contact Enterasys Networks Customer Support as described in Appendix C of this guide.

5

Controlling Remote User Dialing & Access

This chapter describes how to:

- Create or modify a POP Package (a group of ISPs from those available in the TollSaver database) for customized dial-up connections.
- Add or modify corporate ISP information to provide direct dial-up access to the corporate network.
- Add or modify POP information for direct dial-up connections.

NOTE

Destinations, POP Packages and POP phone numbers are included in the Aurorean Client installation kit that you distribute to your remote users. You must perform the steps in this chapter before you can build the custom Aurorean Client installation kit as described in Chapter 6.

Before You Begin

Before performing the steps in this chapter, you should familiarize yourself with the following Aurorean Virtual Network concepts:

- TollSaver database
- Corporate dial-up access
- Problem Notification

TollSaver Database

The TollSaver database contains an extensive list of Point-of-Presence (POP) phone numbers for many Internet Service Providers (ISPs) throughout North America. A master TollSaver database is maintained on the Aurorean Policy Server. To customize this database for your remote users, you simply select the ISPs they are permitted to use from a list and create a *POP package*. When you later build a Aurorean Client installation kit, the APS uses your selections to extract POP phone numbers from the master TollSaver database to build a POP package that is stored on the APS. This custom database is copied onto the remote user's computer when the Aurorean Client installation kit is installed.

You can build as many POP packages as necessary. If you want each group to use a different POP package, you can associate one or more groups with any POP package and build that group's installation kit. Refer to Chapter 6 for more information on building Aurorean Client installation kits.

Because ISPs are constantly opening new POP locations, Enterasys Networks provides a mechanism for updating the master TollSaver database on the APS with new POP phone numbers. The Aurorean Software Update Service delivers periodic TollSaver updates with new ISPs and updated POP phone numbers. Aurorean software updates are normally supplied on a CD ROM which you insert into the APS.

☑ NOTE

For information on the contents of each Aurorean software update and instructions for installing the update, refer to the documentation supplied with the Aurorean Software Update Service CD ROM.

If you select additional ISPs from the database after building a POP package and distributing Aurorean Client installation kits, you can make these ISPs available to your remote users by performing some special steps. These steps include rebuilding the POP package and then enabling client synchronization to download the new ISP POPs to users when they connect. Refer to Chapter 6 for more information on client synchronization.

For instructions on selecting ISPs for your remote clients to use, refer to "Creating POP Packages" on page 105.

Corporate Dial-Up Access

Within RiverMaster, the terms *corporate ISP* and *corporate POPs* are used to describe two types of connections:

- ❐ Direct dial-up remote access to equipment on your corporate network, such as a Windows NT Server equipped with modems and running remote access service (RAS).
- ❐ Tunneled access through an ISP that is not included in the TollSaver database (such as a small, regional ISP that provides your Internet connectivity).

You can integrate phone numbers for these connections into the TollSaver database as corporate POPs. Aurorean Client treats these corporate POP phone numbers no differently from actual POP phone numbers. When the Aurorean Client user enters a From location that is within the local calling area of the direct dial-up equipment or the regional ISP, the corporate POP appears in the list of available POP phone numbers.

To integrate corporate POP phone numbers into the TollSaver database, you first define one or more corporate ISPs. Defining an ISP involves describing its location, entering support contact phone numbers, and corporate network information. You must then add individual corporate POP phone numbers to each corporate ISP. In addition to the phone number, you can choose cost and performance indicators that factor into the *weight* assigned to this method. This weight determines the POPs placement in the dialing list. The POP phone number with the lowest weight is dialed first; if the POP fails to answer the call (for example, if the line is busy), Aurorean Client automatically dials the next POP phone number. By assigning corporate POPs greater weights than standard Internet POPs, you can prevent these direct dial-up connections from being used until all other options are exhausted.

Once you create a corporate ISP, it appears in the list of available ISPs. You then choose the corporate ISP when you select all the ISPs that you want to be part of a POP package. For instructions on defining a corporate ISP for dial-up access, refer to “Adding Corporate ISPs” on page 108. After you define the ISP, you can add individual dial-up POP phone numbers as described in “Adding POPs for Corporate ISPs” on page 114, or, if you wish to gather selected ISPs in a group, you can create a POP package, as described in “Creating POP Packages” on page 105.

Problem Notification

Each Aurorean Policy Server is able to accept reported problems from Aurorean users when they cannot tunnel into the corporate network. The Aurorean Client application issues a Problem Notification when it is unable to build a tunnel while dialing the list of POP phone numbers. Aurorean Client uses RAS to transfer a Prescriber session report detailing the problem to the APS.

The APS' Log Service publishes the session report and stores a problem notification message that can be viewed in the View System Activity pullout (as described in Chapter 7) and within Client Anomaly reports (as described in Chapter 8).

Figure 56 illustrates how the Aurorean Client issues Problem Notifications.

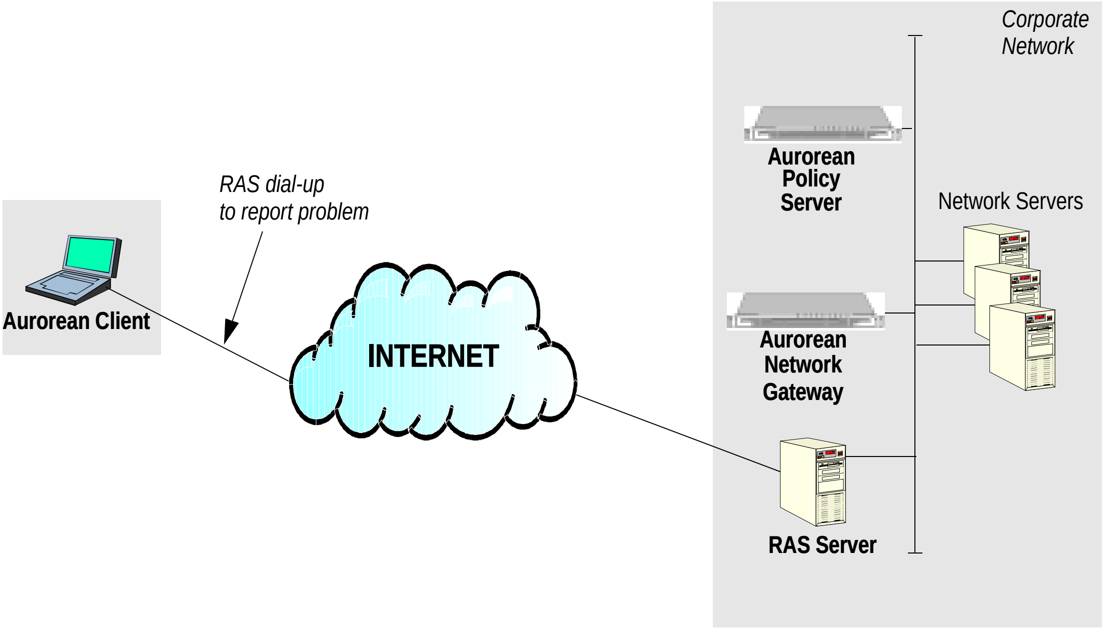


Figure 56 RAS Problem Notification

Creating POP Packages

To configure a POP package, perform the following steps:

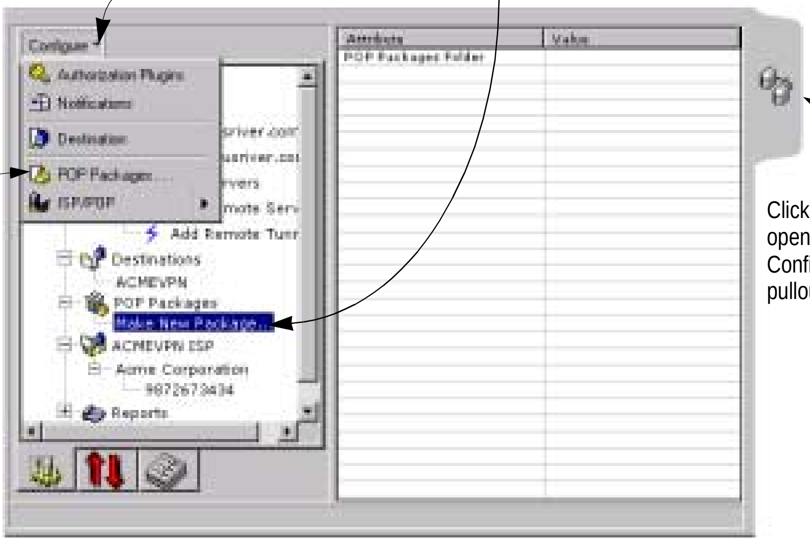
CAUTION

Do not build a POP package while installing or upgrading the APS software - the installation will fail.

1 Open the Configuration pullout.

2 Expand the tree list (click the + symbol) under POP Packages.

The POP Packages display appears similar to the one shown in Figure 57.



Click here to display menu options or here to create a new POP package

Click here to select the POP Packages menu

Click here to open the Configuration pullout

Figure 57 POP Packages Display

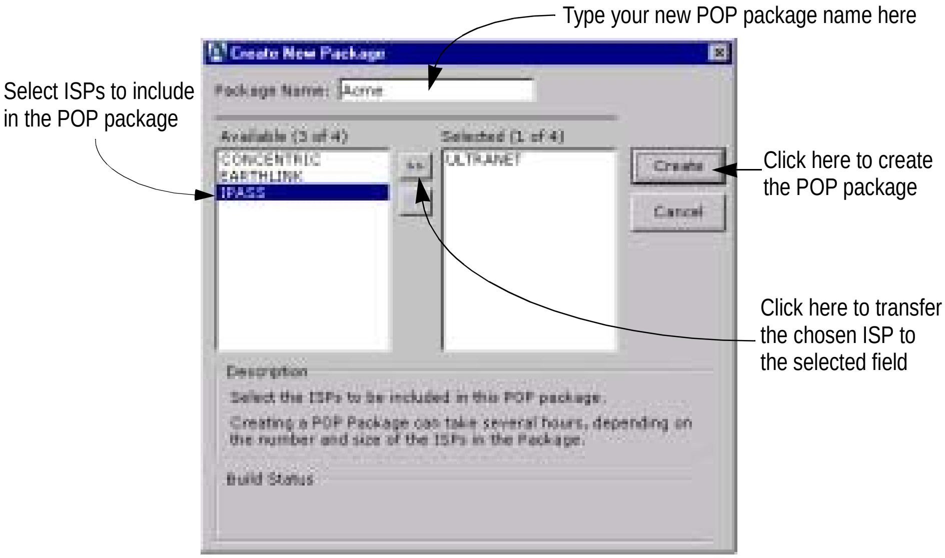
3 Select Make New Package or you may click the arrow next to the Configure menu item at the top left edge of the pullout and select POP Packages.

Either option will display a window similar to the one shown in Figure 58.

4 Select an ISP in the Available list and transfer it to the Selected field by clicking on the double-arrow.

5 Do one of the following:

- Click Create to build the new POP Package.
- Click Cancel to close the window without creating the POP Package.



Create New Package

Package Name: Acme

Available (3 of 4)
CONCENTRIC
EARTHLINK
IPASS

Selected (1 of 4)
ULTRANET

Description

Select the ISPs to be included in this POP package.

Creating a POP Package can take several hours, depending on the number and size of the ISPs in the Package.

Build Status

Type your new POP package name here

Select ISPs to include in the POP package

Click here to create the POP package

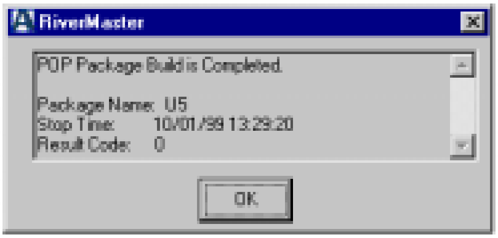
Click here to transfer the chosen ISP to the selected field

Figure 58 Create New Package Display

A message appears indicating the build may take several hours to complete. Also, a trace message indicating the build has started displays in the Message Viewer and, after some time, a trace message indicating the build is complete. You may consult the Attribute area for the selected POP package to check build status.

Even though the creation of POP packages can be lengthy, you can go on to other configuration tasks while the build runs.

6 When the POP package build is completed, a window similar to Figure 59 will display.



```
POP Package Build is Completed.

Package Name:  U5
Stop Time:     10/01/99 13:29:20
Result Code:   0
```

Figure 59 Build Completed Window

NOTE

Creating a POP package is important to enable any Aurorean Client Installation Kit you create later (described in Chapter 6) to dial and allow any users in associated groups (also described in Chapter 6) to synchronize POPs.

Adding Corporate ISPs

To add a new corporate ISP profile, perform the following steps:

1 Open the Configuration pullout.

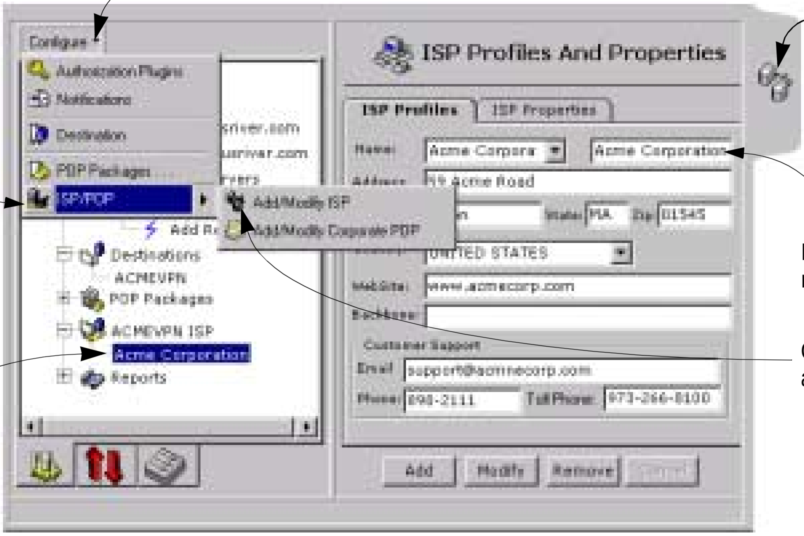
2 Click on the down arrow next to the Configure menu item at the top left edge of the pullout and select POP/ISP from the drop-down menu.

3 Choose Add/Modify ISP from the menu.

The ISP Profiles and Properties display appears similar to the one shown in Figure 60.

NOTE

You can modify information about *any* ISP, corporate or otherwise, within the ISP Profile display.



Name: Acme Corpora ▾ Acme Corporation
Address: 99 Acme Road
State: MA Zip: 01545
UNITED STATES
Website: www.acmecorp.com
Backbone:
Customer Support
Email: support@acmecorp.com
Phone: 898-2111 Toll Phone: 973-266-8100

Click here to display menu options

Click here to display the Corporate ISP menu

Click here to open the Configuration pullout

Enter the ISP's name here

Click here to add the ISP

After you add an ISP, it appears here

Figure 60 ISP Profiles

4 Click on the ISP Profiles tab and then click Add.

5 Type a name for the new ISP in the field next to the Name menu.

This name will appear on the Aurorean Client interface exactly as you typed it. If you are describing a corporate dial-up server, enter a name that identifies your company and the particular server. If you are describing an actual ISP, enter the business name of the ISP.

6 In the Address, City, State, and Zip fields, type the ISP mailing address.

The city and state information will appear on the Aurorean Client interface exactly as you typed it; the remainder of the information is for your reference only.

7 From the Country list, choose the country where the ISP is located.

8 Type the ISP's Web site URL in the Web Site field.

This Web site information will appear on the Aurorean Client interface exactly as you typed it.

9 In the Backbone field, specify the ATM or Frame Relay backbone that serves this ISP (optional).

This information is for your reference only and is not displayed for Aurorean users.

10 In the Customer Support area, type the E-mail address in the E-mail field.

This E-mail address will appear on the Aurorean Client interface exactly as you typed it.

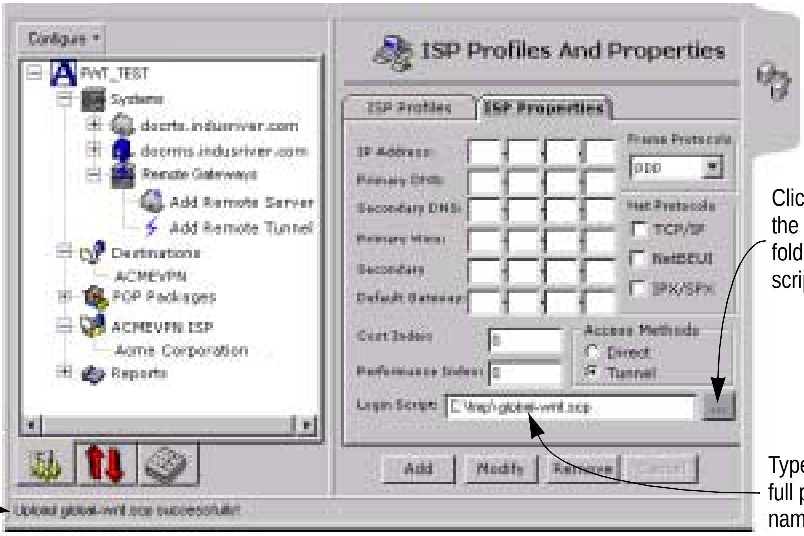
11 In the Phone number field, type the ISP's 800 phone number for technical support.

If the ISP does not have an 800 number support line, enter a local support phone number in the Toll Phone field as described in Step 12.

12 In the Toll Phone field, type the ISP's long distance support phone number.

13 Click the ISP Properties tab.

The ISP Properties display will appear as show in Figure 61.



IP Address: [ ].[ ].[ ].[ ]
Primary DNS: [ ].[ ].[ ].[ ]
Secondary DNS: [ ].[ ].[ ].[ ]
Primary Wins: [ ].[ ].[ ].[ ]
Secondary: [ ].[ ].[ ].[ ]
Default Gateway: [ ].[ ].[ ].[ ]
Frame Protocols: ppp
Net Protocols: □ TCP/IP □ NetBEUI □ IPX/SPX
Cost Index: 0
Performance Index: 0
Access Methods: ○ Direct ● Tunnel
Login Script: C:\tmp\global-vnt.scp

Upload global-vnt.scp successful!!

View messages here

Click here to browse the network for the folder where the script is stored

Type the login script full path or just the name here

Figure 61 ISP Properties

14 In the IP Address field, enter the IP Address of the dial-up server.

If the ISP did not supply this address, you can leave this field blank.

15 In the Primary DNS and Secondary DNS fields, enter the IP addresses of DNS servers used for name resolution.

ISPs normally supply both primary and secondary DNS addresses. For corporate dial-up connections into your network, you must specify at least the primary DNS server’s address.

16 In the Primary WINS and Secondary WINS fields, enter the IP addresses of WINS servers on your network.

ISPs do not typically use WINS for name resolution. If you employ WINS on your network, enter at least one WINS server address (in the Primary WINS field).

17 In the Default Gateway field, enter the IP address of the gateway used to forward packets to other subnets or networks.

18 In the Cost Index field, enter a number between 0 and 999 to indicate the relative cost of using this ISP.

This number is factored into the Weight value that appears on the Aurorean Client interface and affects how POP phone numbers are ordered for dialing. High cost ISPs and their associated POPs appear at the bottom of the list and therefore are dialed last.

19 In the Performance Index field, enter a number between 0 and 999 to indicate the performance cost of this ISP.

This number is factored into the Weight value that appears on the Aurorean Client interface. A high performance index increases the weight associated with the ISP, moving the ISP down the list.

20 Select the Access Method as follows:

– If you are creating a corporate ISP for direct dial-up equipment on your network, select **Direct**. Aurorean users will directly dial into this equipment using the protocol selected from the Frame Protocols list.

✓ NOTE

Direct access does not support Data / Software Synchronization.

– If you are adding a corporate ISP because it does not appear in the TollSaver database, select **Tunnel**. Aurorean users will dial into a POP for this ISP and then negotiate a tunnel into the corporate network.

21 In the optional Login Script field, type the full path of a script file for RiverMaster to locate, optionally using the browse button to search for the directory on your computer where it is stored.

Some ISPs use scripts to enable client login. These scripts are provided by the ISPs, often on their Websites. After you download the script file to your computer, RiverMaster uploads it to the `\IndusRiver\Database\PopScripts` directory on your APS. Later, when you create an installation kit, the login script is incorporated into the management database and built into Aurorean.

✓ NOTE

Script files are not uploaded without the .SCP extension.

22 When the Select New Script Files window appears, click the browse button in the Look in field and find the script you wrote or obtained from your ISP. When finished, click Open.

The Script window appears as shown in Figure 62.

CAUTION

In order for Windows NT logon scripts to run automatically upon connection with Aurorean Client, the following conditions must be met. If all three of the conditions are not complied with, the logon script will not run when a user logs in with Aurorean Client.

- A client computer must be registered on the domain. But, a user need not log into that domain when logging into NT - a user can log in locally to the computer.

- The name of a user logged into NT must match that user's domain login name.

- The user's password on NT must match that user's domain password.

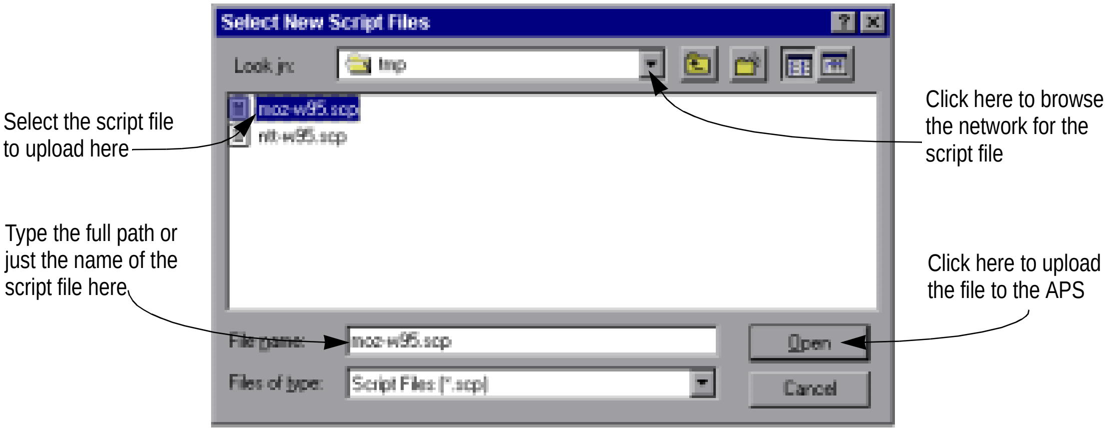

Select New Script Files
Look in:
tmp
moz-w95.scp
nt-w95.scp
File name:
moz-w95.scp
Files of type:
Script Files (*.scp)
Open
Cancel
Select the script file to upload here
Type the full path or just the name of the script file here
Click here to browse the network for the script file
Click here to upload the file to the APS

Figure 62 Select New Script Files Window

23 Choose the dial-up protocols supported by the ISP from the Frame Protocols menu.

Nearly all ISPs and dial-up Remote Access Service (RAS) servers support the default Point-to-Point Protocol (PPP). If the dial-up server at the ISP supports other protocols, such as Serial Line Interface Protocol (SLIP), you may choose another protocol from the menu.

24 Select the Network Protocols to use over the dial-up connection as follows:

– To enable TCP/IP protocol over the dial-up connection, place a check next to TCP/IP. This protocol is required for Internet access.

– To enable Microsoft’s NetBEUI protocol over the dial-up connection, please a check next to NetBEUI. NetBEUI provides fast network browsing in small networks that are primarily Microsoft-based.

– To enable IPX and SPX protocols over the dial-up connection, place a check next to IPX/SPX. These protocols are normally required for access to Novell NetWare servers.

✓ NOTE

NetBEUI is not a routable protocol. You should select at least one other protocol to allow packets to be routed through the Internet or corporate network.

25 Do one of the following:

– Click Update to save the new ISP information.

– Click Cancel to clear the ISP information without saving your changes.

Adding POPs for Corporate ISPs

To add a new POP phone number for a corporate ISP, perform the following steps:

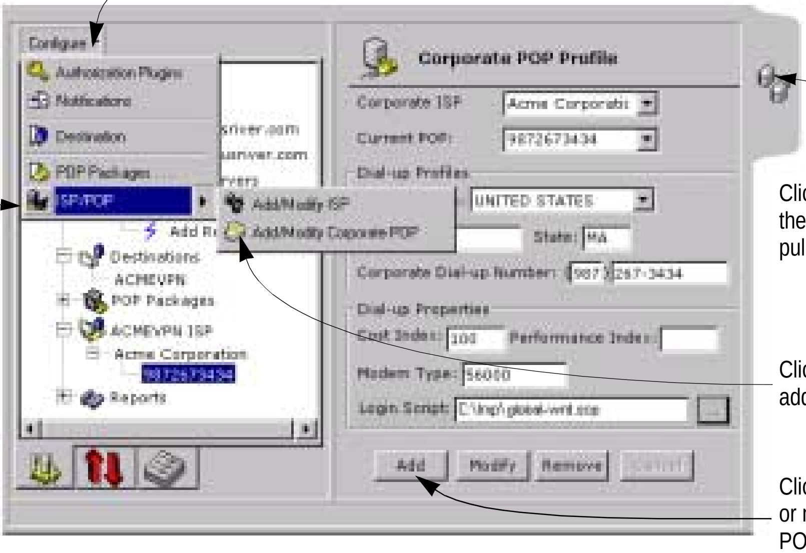
1. Open the Configuration pullout.
2. Click on the down arrow next to the Configure menu item at the top left edge of the pullout.

   The Configure menu items display appears similar to the one shown in Figure 63.
3. Choose ISP/POP from the menu.
4. Choose Add/Modify POP from the menu.

   The Corporate POP Profiles display appears similar to the one shown in Figure 63.

Click here to display menu options

Click here to select the POP menu



Corporate ISP: Acme Corporatic

Current POP: 9872673434

UNITED STATES

State: MA

Corporate Dial-up Number: (987) 267-3434

Cost Index: 100

Performance Index:

Modem Type: 56000

Login Script: C:\tnp\global-vnl.scp

Click here to open the Configuration pullout

Click here to add a POP

Click here to add or modify your POP configuration

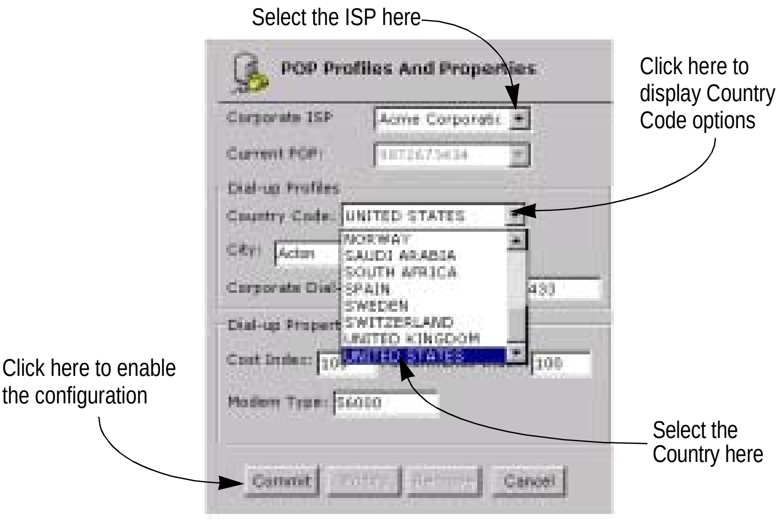
Figure 63 Corporate POP Profiles

5 From the Corporate ISP Name list, choose the ISP that provides the POP or corporate dial-up access.

6 Click Add.

7 In the Country Code field, click the arrow and scroll down the list to select the country where the POP is located.

The pull-down options appear as shown in Figure 64 below.



POP Profiles And Properties

Corporate ISP: Acme Corporati

Country Code: UNITED STATES

City: Acton

Modem Type: 56000

Select the ISP here

Click here to display Country Code options

Click here to enable the configuration

Select the Country here

Figure 64 Country Code Pull-down Options

8 Enter the POP's location in the City and State fields.

The city and state information will appear on the Aurorean Client interface exactly as you typed it.

9 Type the POP or corporate phone number in the Corporate Dial-Up Number fields.

You must enter a full ten digit phone number, including the area code.

10 In the Cost Index field, enter a number between 0 and 999 to indicate the relative cost of using this POP.

This number is factored into the Weight value that appears on the Aurorean Client interface and affects how POP phone numbers are ordered for dialing. High cost POPs appear at the bottom of the list and therefore are dialed last.

11 In the Performance Index field, enter a number between 0 and 999 to indicate the performance history of this POP.

This field is currently not implemented.

12 In the Modem Type field, enter maximum speed of the modem (in bits per second) located at the POP or in the corporate dial-up server.

For example, if the POP offers 56K modem access, type **56000** in this field. The modem type will appear on the Aurorean Client interface exactly as you typed it.

13 In the optional Login Script field, type the full path or just the name of a script file for RiverMaster to locate, optionally using the browse button to search for the directory on your computer where it is stored.

Some corporate ISPs use scripts to enable client login. After you download the script file to your computer, RiverMaster uploads it to the `\IndusRiver\Database\PopScripts` directory on your APS. Later, when you create an installation kit, the login script is incorporated into the management database and built into Aurorean Client.

NOTE

Script files are not uploaded without the .SCP extension.

14 When the Select New Script Files window appears, click the browse button in the Look in field and find the script you wrote or obtained from the ISP. When finished, click Open.

The Script window appears as shown in Figure 65.

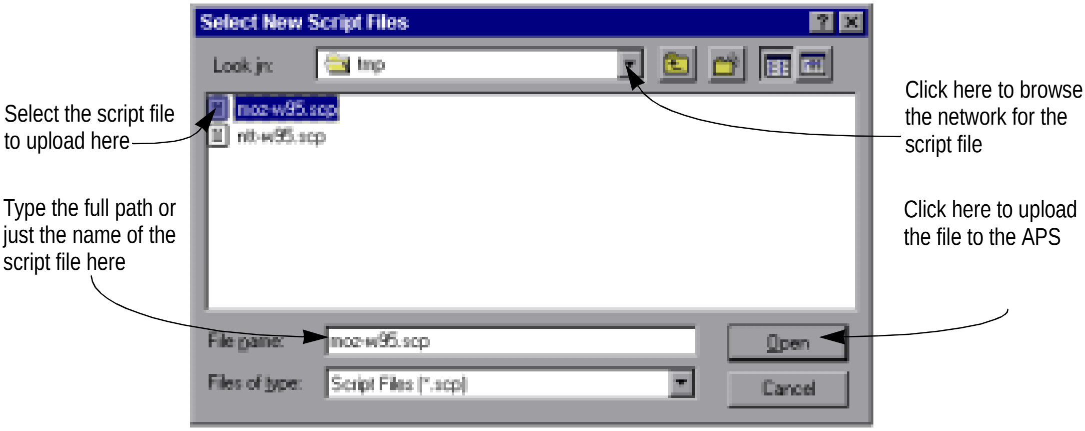

Select New Script Files
Look in:
tmp
moz-w95.scp
nit-w95.scp
File name:
moz-w95.scp
Files of type:
Script Files (*.scp)
Open
Cancel
Select the script file to upload here
Type the full path or just the name of the script file here
Click here to browse the network for the script file
Click here to upload the file to the APS

Figure 65 Select New Script Files Window

15 Do one of the following:

- Click Commit to save the new POP information.
- Click Cancel to clear the POP information without saving your changes.

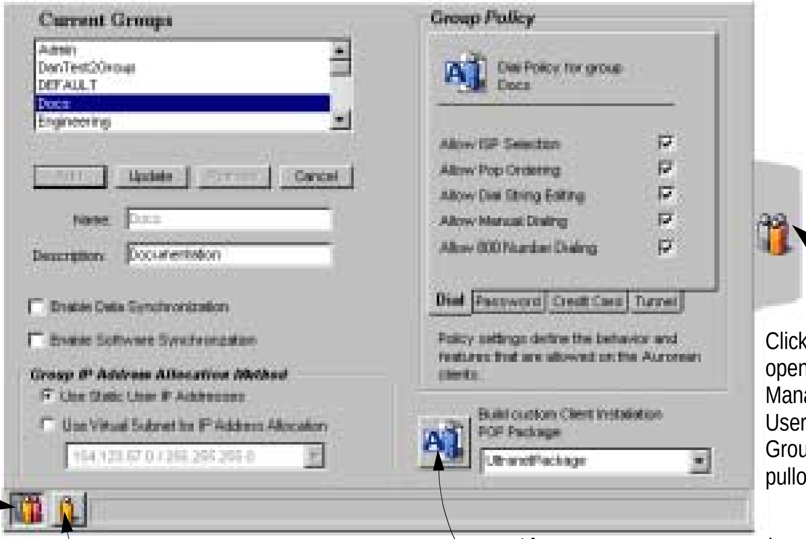
6

Managing Users & Groups

This chapter describes how to:

- ❐ Add, modify, and remove groups from a database residing on the Aurorean Policy Server. Group settings include policies that determine the Aurorean Client features and functions that your remote users are allowed to use.
- ❐ Add, modify, and remove individual user accounts that are used to authenticate remote users via the Enterasys Authorization service.
- ❐ Create a customized Aurorean Client installation kit to distribute to your remote users. This kit contains the Aurorean Client application, group policies, TollSaver POP phone numbers, and destination information.
- ❐ Manage the client synchronization process that automatically updates remote users with policy changes, new POP phone numbers, additional Prescriber remedies, and Aurorean Client application updates each time they connect.
- ❐ Write messages to Aurorean users that they will read when they log in.

The user/group management functions and Aurorean Client installation kit building controls are located on the Manage Users and Groups pullout as shown in Figure 66.



Admin
DanTest2Group
DEFAULT
Docs
Engineering

Name: Docs

Description: Documentation

□ Enable Data Synchronization

□ Enable Software Synchronization

Group IP Address Allocation Method

● Use Static User IP Addresses

○ Use Virtual Subnet for IP Address Allocation

104.123.67.0 / 255.255.255.0

Dial Policy for group
Docs

Allow ISP Selection ☑

Allow Pop Ordering ☑

Allow Dial String Editing ☑

Allow Manual Dialing ☑

Allow 800 Number Dialing ☑

Policy settings define the behavior and features that are allowed on the Aurorean clients.

Build custom Client Installation POP Package

UltranetPackage

Click here to add and modify groups

Click here to open the Manage Users and Groups pullout

Click here to add and modify individual user accounts

After you create a group, assign users and a POP package to that group, click here to create a custom Aurorean installation kit for members of that group

Figure 66 Manage Users & Groups Pullout

Before You Begin

Before performing the steps in this chapter, you should familiarize yourself with the following Aurorean Virtual Network concepts:

- Group policies
- Aurorean Client installation kits
- Client synchronization of the TollSaver database, policy settings, Prescriber remedies and Aurorean Client application updates
- Group Notices

Group Policies

To manage the remote users that will tunnel into your corporate network, you should organize users that share similar access and security needs into groups. For each group, you assign a set of policies that determine the Aurorean Client features and functions that members of that group can use.

Aurorean Virtual Network policies fall into four categories:

- *Dial* policies determine the remote user's control over the POP phone numbers dialed by Aurorean Client. These policies include whether the user can:
  - Change the default order in which POP phone numbers are dialed.
  - Edit the phone number digit string before it is dialed, to add special dialing codes or change the digits.
  - Manually dial the POP phone number using a telephone instead of relying on the modem to generate the digits.
  - Dial a nationwide phone number, such as an 800, 888, or 877 number, instead of a local phone number.
- *Password* policies indicate whether members of this group can save their ISP, corporate ISP and VPN passwords on their Aurorean Client computers, so that they do not need to enter these passwords each time they connect.
- *Credit card* policies specify if users can bill international calls against a calling card and save personal calling card numbers on their Aurorean Client computers, so that they do not need to enter these numbers each time they connect.
- *Tunnel* policies determine the tunneling protocol (IPSec or PPTP) used on all tunnels started by this group's members, whether Firewall / NAT traversal is allowed for Aurorean Client users to reach non-native networks, and whether the IPX protocol can be used over the tunnel to access Novell NetWare servers.

For instructions on setting group policies, refer to "Creating a New Group" on page 127. The policy settings are packaged in the Aurorean Client installation kit that you create for each group as described in the next section. You can change a group's policies after this kit is distributed and installed. The modified policies can be automatically updated on the Aurorean Client computer as described in "Client Synchronization" on page 124.

Aurorean Client Installation Kits

To reduce the challenges of remote access, Enterasys Networks designed Aurorean Client to be embedded with critical access information when it is first installed. Because this information is already present when the remote user tries to connect, the connection occurs quickly and with less chance of error. You are responsible for configuring this information to match your Aurorean Virtual Network requirements, building Aurorean Client installation kits that contain the customized information, and distributing these kits to your remote users.

You must build a Aurorean Client installation kit for each client group defined in the Aurorean Policy Server database. An Aurorean Client installation kit contains the following components:

- ❒ The Aurorean Client application.
- ❒ POP packages, which contain POP phone numbers for the ISPs you selected, as well as any direct dial-up corporate ISP phone numbers.
- ❒ A set of *core files* that contain the following:
  - – The policies assigned to that particular client group. These policies determine which Aurorean Client features and functions users can exercise.
  - – Destination IP address for the Aurorean Network Gateway you want members of that group to access.
  - – The Aurorean VPN name shared by the Network Gateway and Policy servers, and all Aurorean Client computers that connect to your network.

Figure 67 illustrates the contents of a Aurorean Client installation kit.

When you build your first Aurorean Client installation kit, you must perform a complete build. During the two-step build process, the Aurorean Policy Server first extracts POP phone numbers from the master TollSaver database to build a custom database for a POP package and its associated ISPs. If you are using several ISPs or an ISP with POPs nationwide, this POP package build may take a few hours to complete.

In the second step of the build process, a group kit which includes core files containing tunnel, destination, and configuration, is compiled. Compiling this build does not take as long.

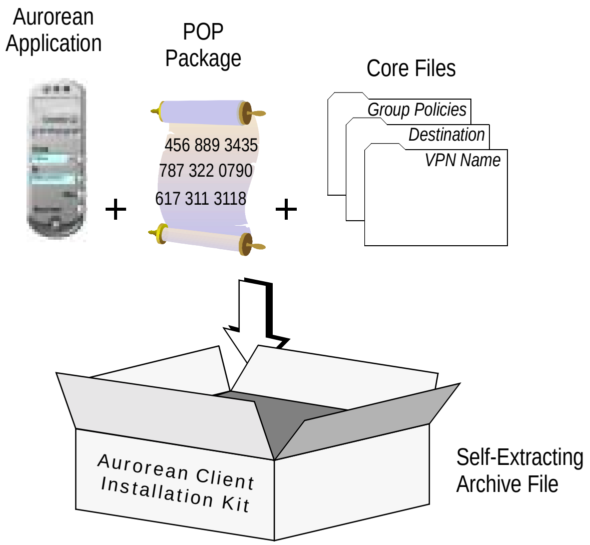


Figure 67 Contents of a Aurorean Client Installation Kit

Once you create a build for one POP package's associated client group, the kits you build for other groups can reuse this customized TollSaver database, reducing the build time. For other groups, you need to build only core files that contain group-specific information (such as policy settings).

During a build, POP packages and core files are generated and stored on the Aurorean Policy Server hard drive. These data files are then packaged in a self-extracting kit file that also contains the Aurorean Client application. The kit file is copied onto your RiverMaster computer into a location of your choosing. Once the file exists on your computer, you are responsible for distributing the kit file to every group member.

For instructions on building a Aurorean Client installation kit, refer to "Creating an Aurorean Client Installation Kit" on page 139.

Client Synchronization

The Aurorean Client installation kit provides your remote users with all the information they need to tunnel into your network for the first time, including ISPs, POP phone numbers, policies, and the IP address of the destination ANG. However, this information may become obsolete if you select additional ISPs, add POP phone numbers, install Aurorean Software Update Service updates, or change the ANG IP address. Using a process known as *client synchronization*, your Aurorean users can receive updated information with a minimum of effort on your part.

Administrator-controlled client synchronization is a two-part process which works by accessing data files (*Data Synchronization*) and software files (*Software Synchronization*) stored on the Aurorean Policy Server. Data files are built when POP package kits or group kits are compiled while the software files consist of pre-standing Aurorean Client application and subsystem executable files. When policies are reconfigured, fresh El Gamal keys created, and new group notices issued, these changes are incorporated in the data files and *automatically* transferred to your Aurorean users through data synchronization (policies are updated every time a user connects). But, other *new* settings including new ISPs and POP packages are *not* transferred during data synchronization unless they have been incorporated in POP package kit and group kit compilations. For those changes to take effect, you must build new POP package and group installation kits for your Aurorean users.

Client synchronization is enabled or disabled on a per group basis. During client synchronization, a portion of the tunnel is taken over as a *management channel* between the Aurorean Client computer and the APS. The management channel operates in the “background” of your connection without any visible effect on connection performance.

The following process occurs each time a Aurorean user establishes a tunnel connection when *both* Data and Software Synchronization are enabled:

1 The APS determines if client synchronization is enabled for a user’s group.

- If data or software synchronization is disabled for that group, no further action is taken.
- If data or software synchronization is enabled for that group, a message appears in the Aurorean Client Prescriber pullout indicating that synchronization has started. A portion of the connection is taken over as the management channel and the process continues with the next step.

2. The APS downloads group policy settings, El Gamal keys, and group notices over the management channel, overwriting the existing policies, keys and notices on the Aurorean Client computer.

   Policy settings are automatically updated on the Aurorean Client computer regardless of whether or not they changed since Aurorean Client was installed and whether or not Software or Data Synchronization is enabled or disabled.

3. With Software Synchronization enabled, Aurorean Client requests new Prescriber scripts and a new version of Aurorean Client from the APS if new scripts and application executable files are available.

   – If new Prescriber scripts are available, the APS begins downloading a self-extracting file over the management channel. This self-extracting file is run the next time the user starts the Aurorean Client application. When the download is complete, the process continues with the next step.
   – If the Prescriber scripts are still current, the process continues with the next step.
   – If new application executable files are available, the APS begins downloading individual files over the management channel. When the download is complete, the process continues with the next step. The new software is installed the next time the user reboots if chosen when prompted by a dialog box. If declined, the user can manually upgrade Aurorean Client later. Also, Aurorean Client replaces any files that were deleted.
   – If the application executable files are still current, the process continues with the next step.
   – If Software Synchronization is disabled, no upgrade occurs.

4. With Data Synchronization enabled, Aurorean Client compares the dates of its most frequently used core and TollSaver POP files against those stored on the APS.

   – If the files are out-of-date, the APS begins downloading individual core and TollSaver POP files over the management channel. When the update is complete, the process continues with the next step.
   – If the files on the Aurorean Client computer are still current, the process continues with the next step.
   – If Data Synchronization is disabled, no upgrade occurs.

5 Aurorean Client requests any remaining core and TollSaver POP files that have changed since Aurorean Client was installed or last synchronized.

– If the files are out-of-date, the APS begins downloading individual core and TollSaver POP files over the management channel. When the update is complete, the process continues with the next step.

– If the files on the Aurorean Client computer are still current, the process continues with the next step.

6 The APS relinquishes the management channel and a message appears on the Aurorean Client Prescriber pullout informing the remote user that synchronization is complete.

✓ NOTE

Prescriber files and Aurorean Client executables downloaded during software synchronization are not immediately available to Aurorean Client users. Users must disconnect the tunnel, *reboot* the PC and restart the Aurorean Client application to put the update files into effect. Files downloaded during data synchronization are available after closing and reopening Aurorean Client .

The Aurorean user can disconnect the tunnel while client synchronization is in progress without causing an error. When the user connects the next time, the APS automatically resumes the transfer of files at the point it was interrupted.

As an alternative to client synchronization, you can also manually create a “patch package” that contains the group’s core files. If an Aurorean user cannot tunnel into the corporate network and you believe the problem is related to outdated group policies or an incorrect ANG destination IP address, you can build and distribute this patch package to that user. Also, if your remote users employ IPSec tunnel protocol and you have regenerated the El Gamal private key on the ANG, you can distribute the patch package to install the new key on their computers. The patch package is a self-extracting archive that automatically overwrites the core files on the Aurorean Client computer. Refer to “Building Core Data Files” on page 147 for instructions on creating a patch package.

For more information on controlling client synchronization, including building new core files and uploading Prescriber remedies, refer to “Controlling Client Synchronization” on page 145.

Group Notices

Administrators may need to notify Aurorean clients of Group-wide news - an upcoming change in policy or a departmental bulletin, for example - and this service is supported by the Group Notice tool. A Group Notice can total 256 characters and can be written for all the clients in a particular group or all members of all groups.

Clients will read the notice in a pop-up Message of the Day box (visible for 30 seconds) upon connecting and the same text will display in their Prescriber pullout as well as their Prescriber log if it is enabled. The notice remains in the Group Notice window until its expiration date. For directions on configuring Group Notices, refer to “Setting Up Group Notices” on page 152.

Creating a New Group

When you first log into RiverMaster, you will observe that one group already exists in the Aurorean Policy Server database: *Admin*, which is the only group that has administrative privileges to log into RiverMaster. This group contains the default login user account (**netadmin**). For administration security, Enterasys Networks recommends that you add a new login account to the Admin group and then remove the Enterasys user account.

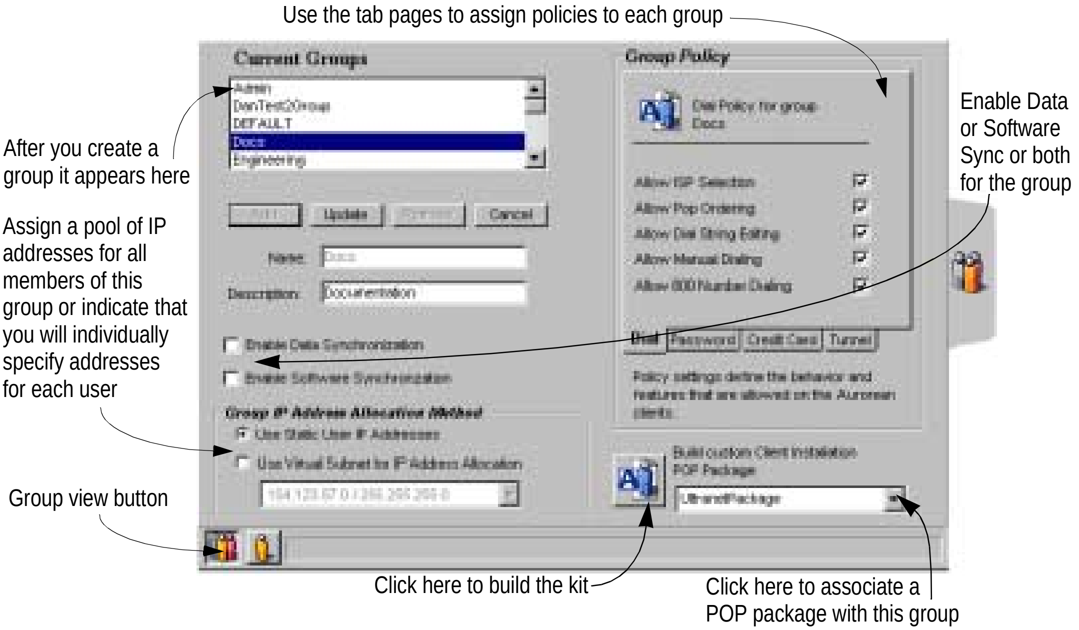
CAUTION

Do not remove the Admin group from the APS database. To log into RiverMaster, you must enter the user name and password of a member of that group. If you remove the group, you will be unable to use RiverMaster in the future.

To create a new group, perform the following steps:

1 Open the Manage Users and Groups pullout.

When you open this pullout, the Group view is automatically displayed as shown in Figure 68.



Use the tab pages to assign policies to each group

After you create a group it appears here

Assign a pool of IP addresses for all members of this group or indicate that you will individually specify addresses for each user

Group view button

Enable Data or Software Sync or both for the group

Click here to build the kit

Click here to associate a POP package with this group

Current Groups: Admin, DanTest2Group, DEFAULT, Docs (selected), Engineering

Name: Docs

Description: Documentation

□ Enable Data Synchronization

□ Enable Software Synchronization

Group IP Address Allocation Method

● Use Static User IP Addresses

○ Use Virtual Subnet for IP Address Allocation

104.123.67.0 / 255.255.255.0

Dial Policy for group Docs

Allow ISP Selection ☑

Allow Pop Ordering ☑

Allow Dial String Editing ☑

Allow Manual Dialing ☑

Allow 800 Number Dialing ☑

Policy settings define the behavior and features that are allowed on the Aurorean clients.

Build custom Client Installation POP Package: UltranetPackage

Figure 68 Manage Users and Groups Pullout - Group View

2 Under the list of Current Groups, click Add.

3 In the Group Name field, enter a name for that group.

For example, if you are structuring groups by department, you can create groups named **Sales**, **Marketing**, and so forth. There is no character limit to Group names, and they may contain letters, numbers, and most symbols. The name you enter appears in the Current Groups list after the group is successfully created.

NOTE

The following symbols are **not** permitted in the Group Name or Description fields: *single* (‘) and *double quote* (“), *space*, *apostrophe* (‘), *tilde* (~), *percent sign* (%), *ampersand* (&), *exclamation point* (!), *backslash* (|), *forward slash* (/), *at sign* (@), and *asterisk* (*).

4 In the Description field, enter information that describes the members of the group.

There is no character limit to descriptions, and they may contain letters, numbers, and most symbols. This field is provided for information purposes only, and does not affect authentication. Only the first 24 characters are shown.

5 To enable client synchronization for this group, begin by selecting Enable Data Synchronization.

When enabled, Data Synchronization automatically provides members of this group with new policy settings, TollSaver POP phone numbers and ISPs whenever they connect. Refer to “Client Synchronization” on page 124 for more information.

6 Complete client synchronization for this group by clicking Enable Software Synchronization.

When Software Synchronization is enabled, any new Prescriber remedies and Aurorean application executable files are provided.

7 Determine how remote users are assigned IP addresses as follows:

- To assign a fixed IP address to each user in this group, select **Use Static User IP Addresses**. When you add a user to this group, you must assign that user a unique IP address as described in “Adding Users to a Group” on page 134.
- To dynamically allocate IP addresses from a pool of addresses, choose a virtual subnet from the **Use Virtual Subnet for IP Address Allocation** list. If this field is blank, you have not defined any virtual subnets; refer to Chapter 3 for instructions on creating virtual subnets.

8 Click the Dial tab and set the group’s dialing policies as described in Table 5 and shown in Figure 68.

Dial policies affect Aurorean users that dial into ISP POPs using analog modems. These policies specify whether those users can change the ISP and POP dialing order, modify a POP phone number before the modem dials it, and manually dial the POP using a telephone.

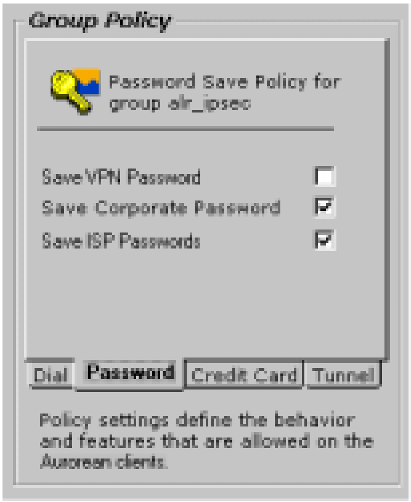
Table 5 Dial Policies

Policy	**Explanation**
Allow ISP Selection	When enabled, Aurorean users can decide whether or not to disable an ISP so that it is not used for dialing. When an ISP is disabled, its associated POP phone numbers do not appear in the dial list. This policy is enabled by default.
Allow POP Ordering	When enabled, Aurorean users can change the dialing sequence for POPs to match their personal preferences. This policy provides the flexibility of mixing POPs of different ISPs as well as moving 800 number POPs ahead of local POP phone numbers. This policy is disabled by default.
Allow Dial String Editing	When enabled, Aurorean users can edit the digit string dialed by their modem, to include any special prefix numbers or other digits required by the telephone equipment at that site. This policy is disabled by default.
Allow Manual Dialing	When enabled, Aurorean users can choose to manually dial a POP phone number using a telephone. With manual dialing, the user’s modem does not send any digits; the user must lift the receiver of a telephone and dial the POP number using the telephone’s keypad. This policy is disabled by default.
Allow 800 Number Dialing	When enabled, Aurorean users can dial a nationwide POP phone number (800, 888, or 877 number) instead of a local phone number. Because ISPs often charge a premium for this type of access, your may want to restrict users from dialing these numbers. This policy is disabled by default.

9 Click the Password tab and set the group’s password policies as described in Table 6 and shown in Figure 69.

Table 6 Password Policies

Policy	Explanation
Save VPN Password	When enabled, Aurorean users can save their VPN password. This password is used while creating the tunnel to authenticate the user against the APS user database or an external RADIUS server. When this policy is disabled, users must retype this information each time they try to tunnel into the corporate network. This policy is disabled by default.
Save Corporate Password	When enabled, Aurorean users can save the password they use for direct corporate network access. When this policy is disabled, users must retype this information each time they try to log into the corporate network. This policy is enabled by default.
Save ISP Passwords	When enabled, Aurorean users can enter and save their password for each ISP they plan to use. The ISP password is used to log the user into the ISP and gain access the Internet. When this policy is disabled, users must retype this information each time they try to log into an ISP. This policy is enabled by default.



Password Save Policy for group alr_ipsec

Save VPN Password □
Save Corporate Password ☑
Save ISP Passwords ☑

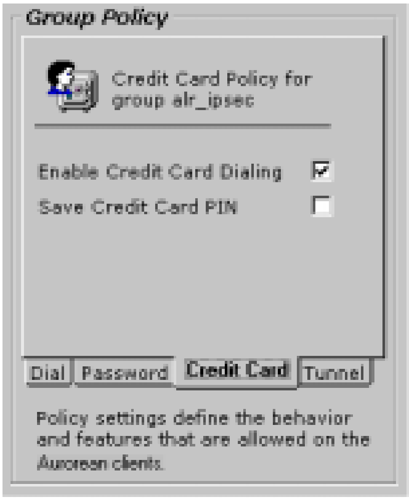
Policy settings define the behavior and features that are allowed on the Aurorean clients.

Figure 69 Password Policies

10 Click the Credit Card tab and set the group’s credit card billing policies as described in Table 7 and shown in Figure 70.

Table 7 Credit Card Policies

Policy	Explanation
Enable Credit Card Dialing	When enabled, Aurorean users can bill long distance or international dial-up connections against a calling card. This policy is enabled by default.
Save Credit Card PIN	When enabled, Aurorean users can save their credit card PIN; this number is stored on the computer in an encrypted format. Enabling this policy saves the remote user time and typing during tunnel setup but at the expense of possible credit card fraud if the user's computer is lost or stolen. This policy is disabled by default.



Credit Card Policy for group alr_ipsec

Enable Credit Card Dialing ☑
Save Credit Card PIN □

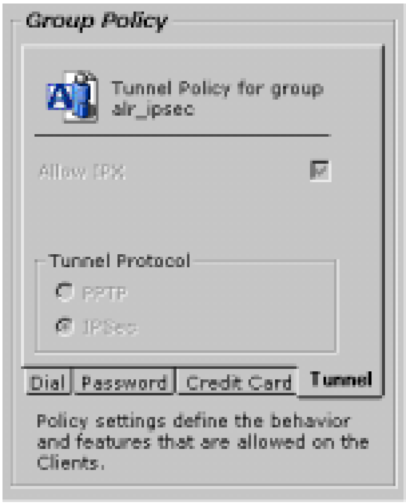
Policy settings define the behavior and features that are allowed on the Aurorean clients.

Figure 70 Credit Card Policies

11 Click the Tunnel tab and set the group's tunnel policies as described in Table 8 and shown in Figure 71.

Table 8 Tunnel Policies

Policy	Explanation
Allow IPX	When enabled, Aurorean Client negotiates IPX protocol with the ANG and the user can access Novell NetWare servers on the network. This policy is disabled by default.
Allow Firewall Traversal	When enabled, Aurorean Client traverses firewalls or NAT servers to successfully connect with the ANG. This policy is disabled by default. Firewall/NAT traversal employs the HyperText Transfer Protocol - Secure (HTTPS) to encapsulate the selected tunneling protocol (IPSec or PPTP) and thereby prevent a firewall or NAT server from blocking Aurorean Client's return connection to the computer where the application resides.
Tunnel Protocol	Determines which tunneling protocol, Point-to-Point Tunneling Protocol (PPTP) or Internet Protocol Security (IPSec), is used on all tunnels started by users in this group. The default tunneling protocol is PPTP.



Group Policy

Tunnel Policy for group air_ipsec

Allow IPX ☑

Tunnel Protocol

○ PPTP

● IPSec

Policy settings define the behavior and features that are allowed on the Clients.

Figure 71 Tunnel Policies

NOTE

If you allow IPX, rebuild the client kit for that group after setting this policy, then have your users uninstall their old Aurorean Client and install the new Aurorean Client. Client synchronization does not support this change.

12 Do one of the following:

- Click Commit to store the new group name on the APS.
- Click Cancel to cancel the operation.

Adding Users to a Group

To add a user to a group, perform the following steps:

NOTE

You only need to add user accounts when using the Authorization service. If you disabled Authorization in favor of authenticating users against a RADIUS or SecurID server, you do not need to create accounts for your remote users. Refer to Chapter 4 for more information on Aurorean Virtual Network authentication techniques.

1 Open the Manage Users and Groups pullout.

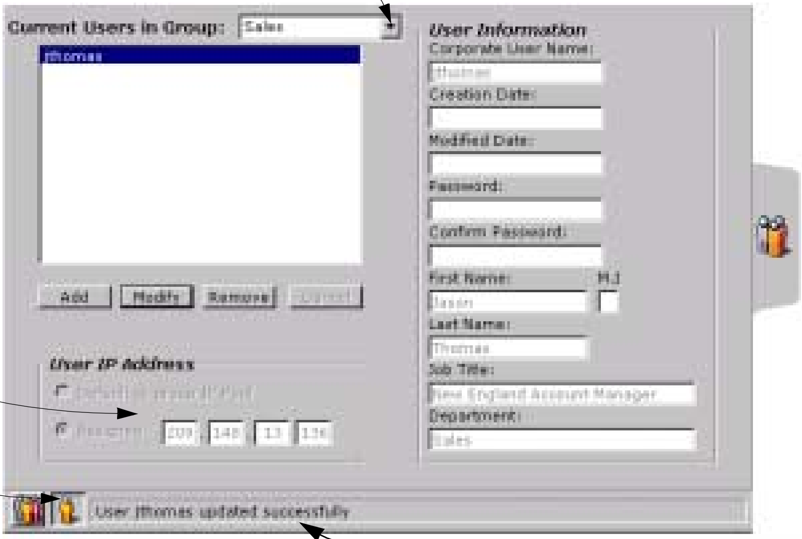
2 Click on the User icon in the lower left corner of the pullout to switch to the User view.

A sample User view is shown in Figure 72.

Click here to choose the group you want the user to join

Use these fields to assign a static IP address to the user or dynamically allocate an IP address from the group's virtual subnet

Individual view button



Current Users in Group: Sales

jthomas

User IP Address

○ Default to Group IP Pool
● Assigned 209 . 148 . 13 . 136

User Information

Corporate User Name: jthomas

Creation Date:

Modified Date:

Password:

Confirm Password:

First Name: Jason M.I.

Last Name: Thomas

Job Title: New England Account Manager

Department: Sales

User jthomas updated successfully

Progress messages appear here

Figure 72 Manage Users and Groups Pullout - User View

3 From the Group list, choose the group you want the user to join.

4 Under the list of Current Users, click Add.

5 In the User IP Address fields, select how the user receives an IP address when he or she connects to the network over a tunnel.

- To allocate the user an IP address from the virtual subnet assigned to this group, select **Default to Group IP Pool**.
- To assign the user a specific address that is used every time the user connects, select **Assigned** and enter an IP address and subnet mask in the fields provided.

6 In the Corporate User Name field, type a name for the user.

There is no character limit to User names and they may contain letters, numbers, and most symbols. This name matches the VPN User Name that remote users must enter to use Aurorean Client.

NOTE

The following symbols are **not** permitted in the Corporate User Name field: *single (‘)* and *double quote (“), space, apostrophe (‘), tilde (~), percent sign (%), ampersand (&), exclamation point (!), backslash (|), forward slash (/), at sign (@),* and *asterisk* (*).

7 In the Password field, type a unique password.

Passwords are not limited in character length and may contain letters, numbers or symbols.

8 In the Confirm Password field, retype the same characters you entered in the Password field.

Passwords are case-sensitive, so you must enter the characters exactly as you typed them in the Password field.

9 In the First Name, M.I., and Last Name fields, type the user’s first and last name, and middle initial (optional).

This information is used for reference only and has no effect on authentication.

10 In the Job Title and Department fields, type information to describe the user’s position in the company (optional).

The Department field automatically defaults to the group name.

11 Do one of the following:

- Click Commit to store the new user account on the Aurorean Policy Server.
- Click Cancel to cancel the operation.

Modifying User & Group Information

After a user or group has been created, you can modify any setting associated with the user or group name, including group policies, IP address allocation methods, and user passwords. Although you cannot rename a user or group, you can accomplish the same goal by removing the user or group and then reentering the information using a new name.

To modify user or group information, perform the following steps:

1. Open the Manage Users and Groups pullout.
2. Click on the appropriate icon in the lower left corner of the pullout to select the Group or User view.
3. Select the user or group name from the list of Current Users or Current Groups.
4. Click Modify.
5. Change the settings for the user or group as required.
6. Do one of the following:
   - Click Update to put your changes into effect.
   - Click Cancel to return the user or group information to its original state.

The modified information is immediately saved on the APS.

NOTE

Any changes made to Group Policies are conveyed to users *automatically* through Client Synchronization regardless of whether Data or Software Synchronization are enabled or not.

Removing Users & Groups

CAUTION

Do not remove the Admin group from the APS database. To log into RiverMaster, you must enter the user name and password of a member of that group. If you remove the group, you will be unable to use RiverMaster in the future.

To remove a user or group from the APS, perform the following steps:

1. Open the Manage Users and Groups pullout.
2. Click on the appropriate icon in the lower left corner of the pullout to select the Group or User view.
3. Select the user or group name from the list of Current Users or Current Groups.
4. Click Remove.
5. When a confirmation window appears, do one of the following:
   - Click OK to immediately remove the group from the APS database.
   - Click Cancel to leave the group intact on the APS.

Creating an Aurorean Client Installation Kit

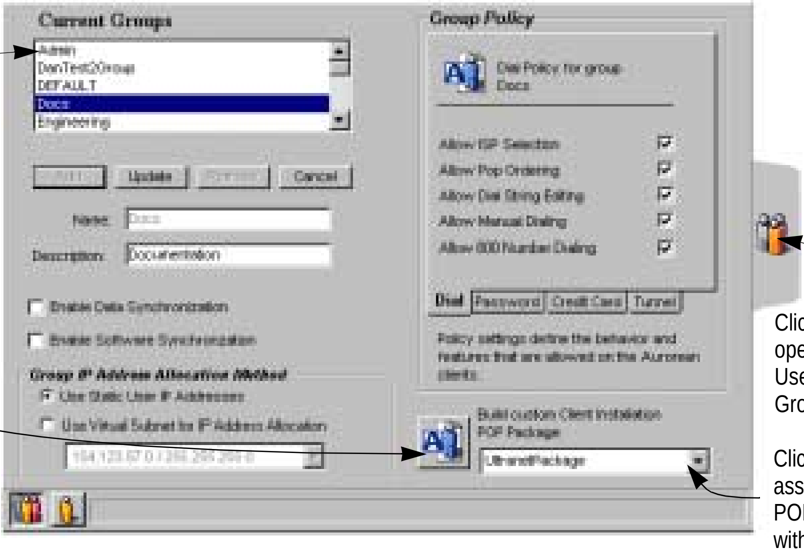
To build a Aurorean Client installation kit for a group, perform the following steps:

NOTE

While the installation kit is built, client synchronization is disabled for that group. You must manually re-enable Data Synchronization after the build is complete in order for group members to receive TollSaver database or policy updates or re-enable Software Synchronization to disburse new Prescriber scripts and an updated Aurorean application.

1 Open the Manage Users and Groups pullout.

A sample Group view is shown in Figure 73.



Current Groups

Admin
DanTest2Group
DEFAULT
Docs
Engineering

Name: Docs
Description: Documentation

□ Enable Data Synchronization
□ Enable Software Synchronization

Group IP Address Allocation Method
● Use Static User IP Addresses
○ Use Virtual Subnet for IP Address Allocation

Group Policy

Dial Policy for group Docs

Allow ISP Selection ☑
Allow Pop Ordering ☑
Allow Dial String Editing ☑
Allow Manual Dialing ☑
Allow 800 Number Dialing ☑

Policy settings define the behavior and features that are allowed on the Aurorean clients.

Build custom Client Installation
POP Package
UltranetPackage

Select the group from here

Click here to start building the kit

Click here to open the Manage Users and Groups pullout

Click here to associate a POP package with a kit

Figure 73 Starting the Kit-Building Process

2 In the Current Groups list, select the group for which you are creating the installation kit. If you will be selecting a different POP Package than is displayed in the field next to the Build Custom Installation Kit button, click Modify; otherwise, go to Step 3.

3 In the field next to the Build Custom Installation kit button, click the browse arrow and choose a POP package to associate with the selected group. Click Update.

If you have not already built a POP package, refer to Chapter 5, “Creating POP Packages”, for instructions.

4 Click the Build Custom Installation kit button.

5 When the Build Client Install Kit window appears, use the Output Directory field to specify where the resulting installation kit file should be stored on your computer.

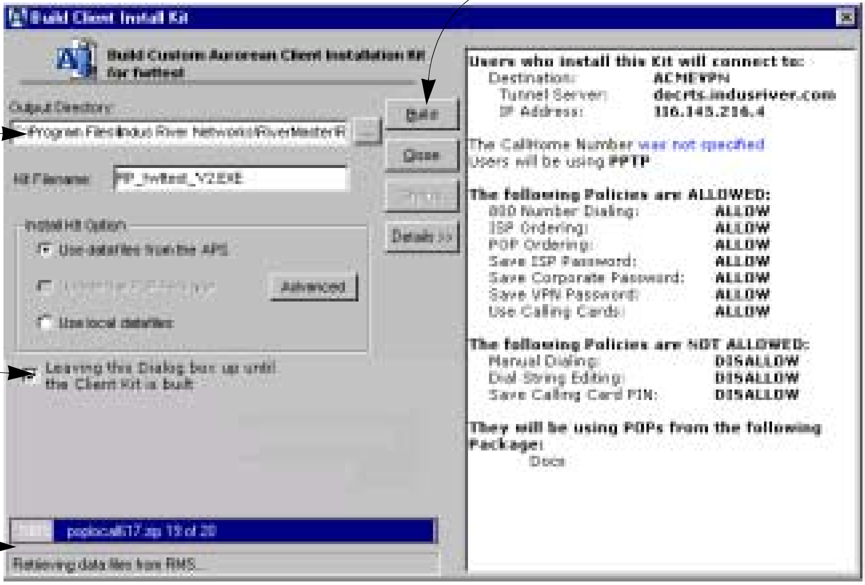
A sample window is shown in Figure 74. The default destination for Aurorean installation kit files is `C:\Program Files\Indus River Networks\RiverMaster\RiverPilot_Packages`. To change the output directory, click the button to the right of the field and use the Open window to select or create another directory.

Specify where you want the resulting installation kit file stored on your computer here

Leave this box checked to receive progress messages as the kit is built

Progress messages appear here as the kit is built

Click here to start the build



Build Client Install Kit

Build Custom Aurorean Client Installation Kit for Twitest

Output Directory: C:\Program Files\Indus River Networks\RiverMaster\R

Kit Filename: PP_twitest_V2.EXE

Install Kit Option

● Use datafiles from the APS

○ [illegible]

○ Use local datafiles

☑ Leaving this Dialog box up until the Client Kit is built

poplocal617.zip 19 of 20

Retrieving data files from RMS...

```
Users who install this Kit will connect to:
  Destination:                ACMEVPN
   Tunnel Server:             decrts.indusriver.com
   IP Address:                116.145.216.4

The CallHome Number was not specified
Users will be using PPTP

The following Policies are ALLOWED:
  800 Number Dialing:             ALLOW
  ISP Ordering:                   ALLOW
  POP Ordering:                   ALLOW
  Save ISP Password:              ALLOW
  Save Corporate Password:        ALLOW
  Save VPN Password:              ALLOW
  Use Calling Cards:              ALLOW

The following Policies are NOT ALLOWED:
  Manual Dialing:                 DISALLOW
  Dial String Editing:            DISALLOW
  Save Calling Card PIN:          DISALLOW

They will be using POPs from the following
Package:
        Docs
```

Figure 74 Build Client Install Kit Window

6 In the Kit Filename field, specify a name for the self-extracting Aurorean installation kit file.

The default Aurorean installation kit file name is

RP_*Group*_*Release#*.EXE

where *Group* indicates which group policies are applied to the Aurorean application and *Release#* specifies the version of Aurorean included in the kit (for example, V3 indicates Aurorean Release 3.0). You can modify the file name to suit your needs, but do not change the .EXE file extension.

7 Set the Install Kit Options as follows:

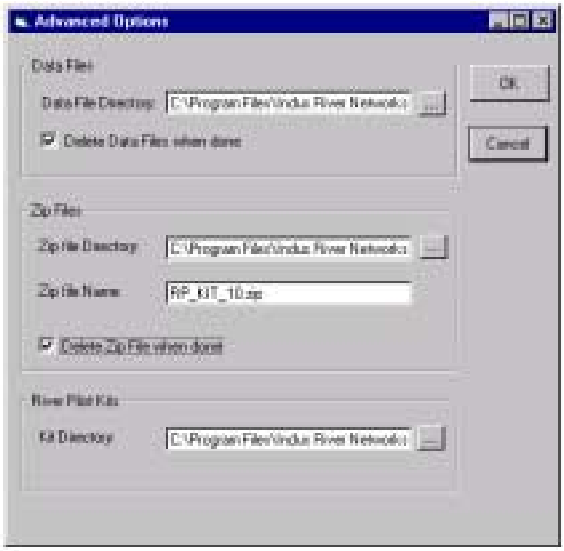
- The first time you build a kit, the only option available will be **Use datafiles from the APS**. This choice retrieves POP phone numbers from the **APS**. After you have built your first kit, choosing this option is useful if you have added more ISPs or POP phone numbers to your POP package and want to update your configuration.
- To generate a revised TollSaver database from files on the **APS** (the slowest kit-building option), select **Update the POP Package**. This option is available only after you build your first kit.
- To use an existing customized TollSaver database already stored on your RiverMaster computer from a previous build (the fastest kit-building option), select **Use local datafiles**. This option is available only after you build your first kit.

8 To leave this window open on your desktop until the kit completes, place a check next to Leaving this Dialog box up until the Client Kit is built.

While the kit is built, progress messages appear at the bottom of this window.

9 Do one of the following:

- To use the default directories for storing and retrieving data, ZIP, and Aurorean application files on your computer (recommended), skip to Step 14.
- To modify the directories used to store and retrieve data, ZIP, and Aurorean application files on your computer, click Advanced and continue with the next step. Selecting this option will display a window similar to Figure 75.



Data File Directory: C:\Program Files\Indus River Networks

☑ Delete Data Files when done

Zip file Directory: C:\Program Files\Indus River Networks

Zip file Name: RP_KIT_10.zip

☑ Delete Zip File when done

Kit Directory: C:\Program Files\Indus River Networks

Figure 75 Advanced Kit Options Window

10 In the Data Files area, specify the destination directory on your computer for POP phone number data files and indicate whether you want the data files preserved or deleted after the kit is built.

POP data files for each area code are created on the **APS** and then copied to the RiverMaster computer. You can choose to delete these files once they are included in the installation kit or preserve the files for future kits (allowing you to select the Use Existing Data Files kitting option).

11 In the Zip Files area, specify the destination directory and file name for the Zip file used in the self-extracting archive and indicate whether you want the Zip file preserved or deleted after the kit is built.

12 In the Aurorean Client Kits area, specify the source directory of the Aurorean application you want to distribute.

By default, Aurorean is copied into `C:\Program Files\Indus River Networks\RiverMaster\ RiverPilotKits` when you install RiverMaster. Aurorean Client files are stored in directories named after the software's version number (for example, the Version 3 directory contains Aurorean Software Release 3.0 software). If you are maintaining different releases of Aurorean among your users, indicate which version you want to distribute by selecting the appropriate directory.

13 Click OK to close the Advanced Options window and save your changes.

14 On the Build Client Install Kit window, click Build to start creating the installation kit.

If you choose to leave this window open during the build, real-time messages appear at the bottom of the window indicating build status.

NOTE

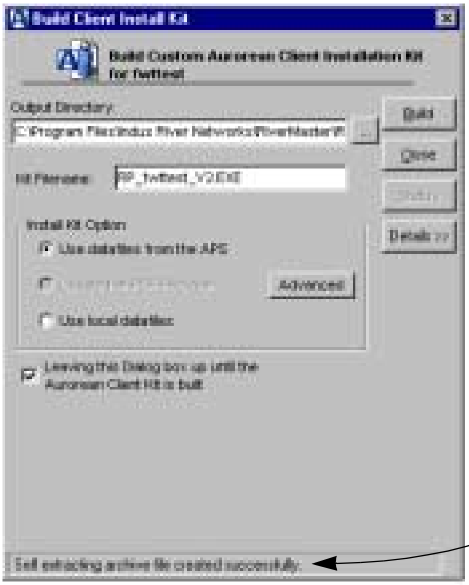
If problems are detected early in the build process, (for instance, a POP package was not created), the details screen of the Build Client Install Kit window will display the problem in red, suggesting what should be fixed before proceeding with the build.

15 If you are building a kit for the first time or you specified directories that do not currently exist, a series of windows appear asking if you want to create each directory; click Yes at each window to create the new directories.

After the directories are created, RiverMaster copies the POP data files onto your computer and starts generating the ZIP file and overall self-extracting archive file. Progress messages appear on the Build Client Install Kit window (if you chose to leave it open) as these actions occur.

16 If you opt to keep the Build Client Install Kit window open during the build, a message appears at the bottom of the window when the build completes as shown in Figure 76; click Close to close the window.

An Access message indicating the build completed also displays in the Message Viewer. Additional build information is available by choosing the POP Package and examining its Attributes and Values as shown in Chapter 5.



C:\Program Files\Induz River Networks\RiverMaster\P

Kit Filename: RP_twftest_V2.EXE

● Use data files from the APS

○

○ Use local data files

☑ Leaving this Dialog box up until the Aurorean Client Kit is built

Self extracting archive file created successfully.

This message indicates the installation kit was successfully built

Figure 76 Kit Complete Message

Check the output directory to view the installation kit file. You must copy the file to a network file server or high-capacity media (such as a ZIP disk) to distribute the installation kit to your users.

NOTE

To install the Aurorean Client installation kit, refer to the *Aurorean Client User's Guide*, *Aurorean Client Quick Reference Card*, or *Aurorean Client Release Notes.*

Controlling Client Synchronization

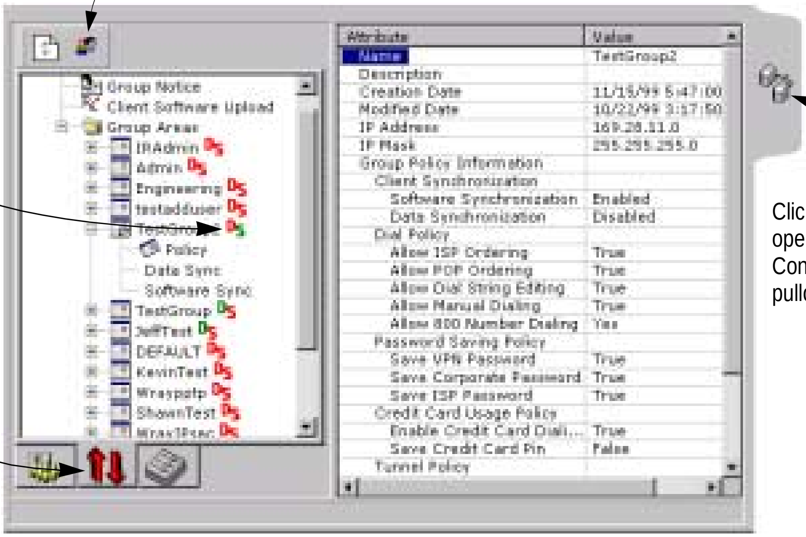
After you enable client synchronization for a group and distribute Aurorean Client installation kits to its members, you can manage the process of updating these clients in these ways:

- ❐ View a summary of each group’s current policies
- ❐ Build new Aurorean Client core data files that contain policy settings, destination Aurorean Network Gateway IP address, and other critical access information
- ❐ Upload new Prescriber remedies and the updated Aurorean Client program to the **APS** from a Aurorean Software Update Service update CD ROM
- ❐ Communicate to all Group members via Group Notice

These functions are available by opening the Configuration pullout and clicking on the Update tab as shown in Figure 77.

Green **D** (data) or **S** (software) indicates what type of sync is **enabled**. Red **D** (data) or **S** (software) shows what type of sync is **disabled** for this group

Click here to view the Build Aurorean Client Core Data Files display



Attribute	Value
Name	TestGroup2
Description	
Creation Date	11/15/99 5:47:00
Modified Date	10/22/99 3:17:50
IP Address	169.28.11.0
IP Mask	255.255.255.0
Group Policy Information	
Client Synchronization	
Software Synchronization	Enabled
Data Synchronization	Disabled
Dial Policy	
Allow ISP Ordering	True
Allow POP Ordering	True
Allow Dial String Editing	True
Allow Manual Dialing	True
Allow 800 Number Dialing	Yes
Password Saving Policy	
Save VPN Password	True
Save Corporate Password	True
Save ISP Password	True
Credit Card Usage Policy	
Enable Credit Card Diali...	True
Save Credit Card Pin	False
Tunnel Policy	

Click here to open the Configuration pullout

Click here to view the client update options

Figure 77 Client Synchronization Controls

Viewing Group Policies

To view a summary of each group’s policy settings, follow these steps:

1 Open the Configuration pullout.

2 Click the Update tab.

3 In the Global Area, expand the tree list under Group Areas (click the + symbol).

4 Expand the tree list under the name of the group you want to view.

A **D** next to the group name symbolizes Data Synchronization, an **S** stands for Software Synchronization. Green indicates synchronization is turned on, red indicates it is turned off. See Figure 77 for examples.

The current policy settings are displayed in the window pane to the right. If data or software synchronization is enabled for that group, the settings displayed are automatically overwritten on the Aurorean Client computer whenever members of that group tunnel into the corporate network. To change these policy settings, refer to the instructions in “Modifying User & Group Information” on page 137.

5 To refresh the policy display, click the Refresh button located in the toolbar at the top edge of the pullout.

6 To enable client synchronization for a group at any time, right-click on the group name, select Data or Software Synchronization, and click Enable Data or Software Sync as shown in Figure 78.

You can also enable the service on the Manage Users and Groups pullout as described in “Creating a New Group” on page 127. You can disable the service by right-clicking on the group name, clicking on Data or Software Synchronization, and clicking Disable Data or Software Sync; alternatively, you can uncheck either of the synchronization boxes in the Manage Users and Group pullout.

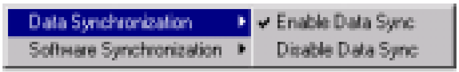


Figure 78 Data and Software Synchronization Dialog Boxes

Building Core Data Files

Typically, you build new sets of core data files in the following situations:

- If you have changed the IP address for the External port on the ANG.
- If you encounter configuration-related problems that prevent Aurorean users from connecting and receiving new policy and Prescriber updates using the normal Client Synchronization method.
- If you have regenerated the El Gamal private/public keys required by IPSec clients to tunnel into the corporate network (refer to Chapter 4 for more information on generating these keys).

To build new core data files, perform the following steps:

1 Open the Configuration pullout.

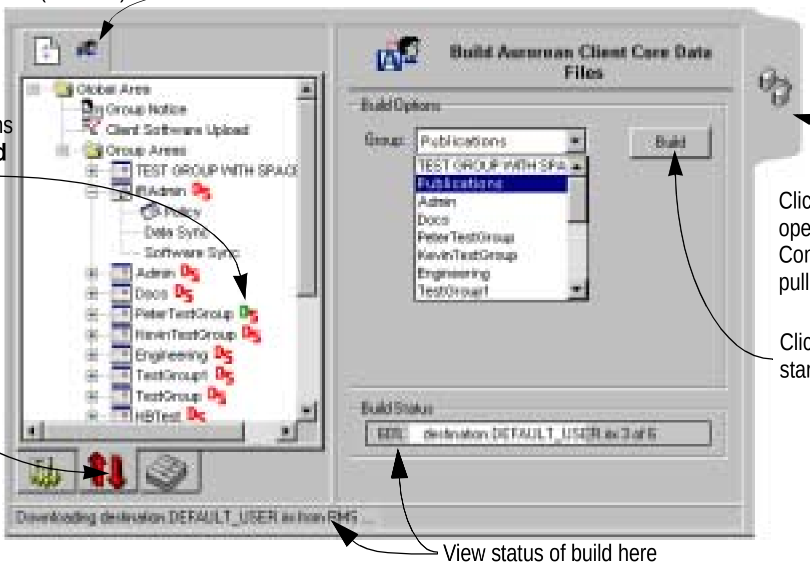
2 Click the Update tab.

3 Choose Build Patch Program from the toolbar on the top edge of the pullout.

Figure 79 shows the Configuration pullout with the Build Aurorean Client Core Data Files display selected.

Green **D** (data) or **S** (software) indicates what type of sync is **enabled**. Red **D** (data) or **S** (software) means sync is **disabled** for this group

Click here to view the Build Aurorean Client Core Data Files display



Group: Publications

60% destination DEFAULT_USER.ini 3 of 5

Downloading destination DEFAULT_USER.ini from RMS ...

Click here to view the client update options

Click here to open the Configuration pullout

Click here to start the build

View status of build here

Figure 79 Build Core Data Files Display

4 From the Group menu, choose the group you want to receive the new set of core data files.

5 Click Build.

As the core files are built, status messages appear in the lower left corner of the pullout and in the Build Status area.

6 If you have not previously built core files for this group, a Directory Not Found window appears asking you to create a new directory for the core files; click Yes to create the directory.

If you installed RiverMaster in the default location on your computer, the new core files are stored in `C:\Program Files\Indus River Networks\RiverMaster\DataFiles\RiverPilot\`*`GroupName`* where *GroupName* is a subdirectory that matches the group name.

The new core files are also maintained on the APS. If client synchronization is enabled for the group, members of the group automatically receive the updated files during synchronization.

To manually distribute the new core files to users who cannot connect, copy the contents of the directory created in Step 6 onto a floppy disk or other distributable media. Aurorean users must copy these .IRX files into the Data directory on their computers (by default, `C:\Program Files\Indus River Networks\RiverPilot\Data`).

NOTE

After Aurorean users copy the new core files onto their computers, they must re-enter their VPN and ISP user names and passwords. Any From locations they added are preserved and do not need to be reentered.

Uploading Software Synchronization Files

New Prescriber remedies and updated Aurorean Client application files are distributed as part of Enterasys Network’s Aurorean Software Update Service. In order for Aurorean clients to receive this information, a set of files containing the scripts and application executables as well as a table of contents file (`rx-toc.txt`) must be uploaded to the APS. Once the files are uploaded, Aurorean clients automatically receive the new Prescriber remedies and revised Aurorean Client program files through the software synchronization process.

NOTE

You must enable software synchronization for each group in order for Aurorean users to automatically receive new Prescriber and Aurorean Client application files. Refer to page 146 for directions to enable software synchronization.

To upload new software synchronization files, perform the following steps:

1 Open the Configuration pullout.

2 Click the Update tab.

3 Expand the list under Global Area.

4 Click the Upload icon.

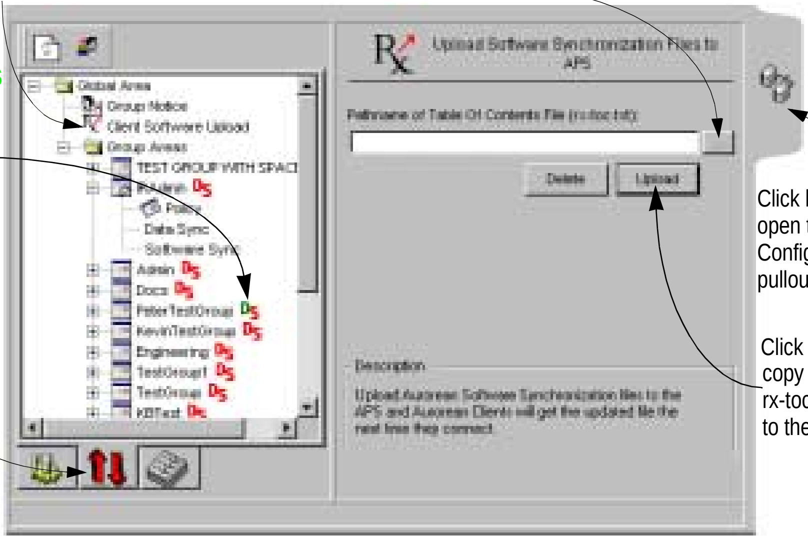
The Upload Software Synchronization Files to APS display appears as shown in Figure 80.

Click here to view the Upload software synchronization files to APS display

Click here to browse for the software synchronization file (rx-toc.txt) file

Green **D** (data) or **S** (software) indicates what type of sync is **enabled**. Red **D** (data) or **S** (software) shows the type of sync **disabled**

Click here to view the client update options



Upload Aurorean Software Synchronization files to the APS and Aurorean Clients will get the updated file the next time they connect.

Click here to open the Configuration pullout

Click here to copy the rx-toc.txt file to the APS

Figure 80 Upload Software Synchronization Files Display

...

5 Select the directory where the new software sync files reside by clicking the browser.

In addition to Software Synchronization files (Prescriber remedies and Aurorean Client executables), a table of contents file (`rx-toc.txt`) is transferred to the APS. This text file lists all the synchronization files contained in the ZIP file and is used during client synchronization to determine if the Aurorean user requires new software files.

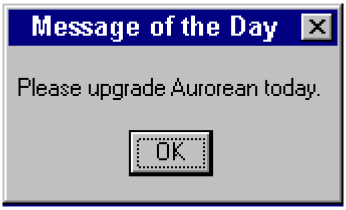
6 Click Upload to copy the file you chose onto the APS.

The Software Synchronization files are copied into the `C:\Program Files\Indus River\Scripts\Java` directory on the APS. Software Synchronization and `rx-toc.txt` files must be located in the same directory for successful uploading.

During client synchronization, Aurorean Client compares its `rx-toc.txt` file against the version you uploaded. If new software files are available, the APS downloads them over the management channel. When the Aurorean user starts the Aurorean Client application the next time, the new software files are immediately available for use.

Setting Up Group Notices

Group Notices can be written to notify Aurorean users in each group or all Aurorean users in a global message. The notice displays in a standard pop-up window as shown in Figure 81 below. The message disappears after 30 seconds or when the user clicks OK.



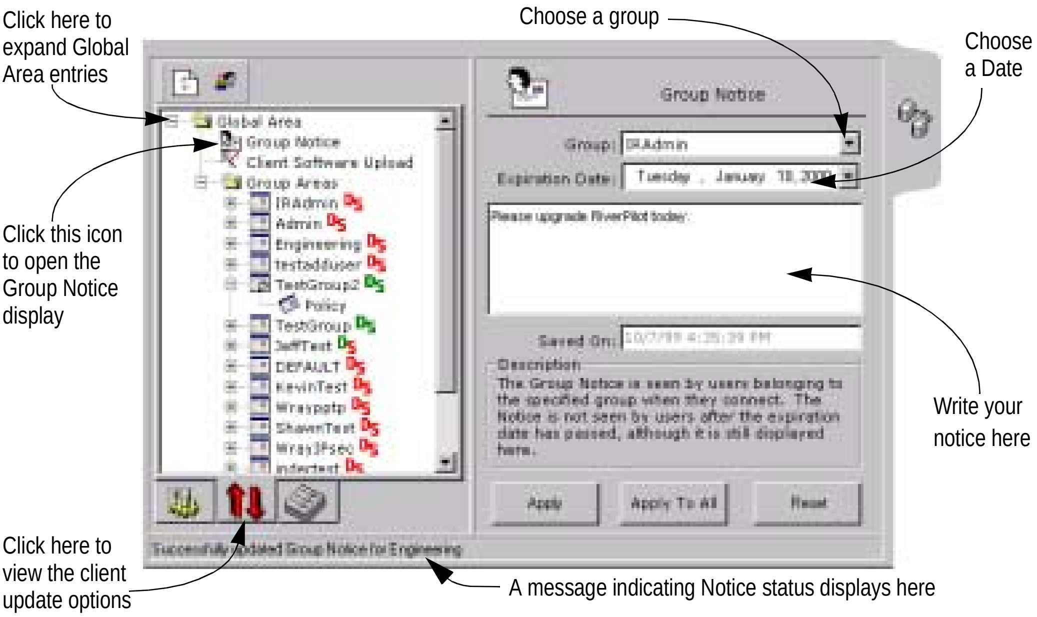
Please upgrade Aurorean today.

Figure 81 Group Notice Display

To write messages for clients in a single Group or all-Group basis, perform the following steps:

1. Open the Configuration pullout.
2. Click the Update tab.
3. Expand the tree list under Global Area.
4. Click on the Group Notice icon.

   The Group Notice display appears as shown in Figure 82.



Group: IRAdmin

Expiration Date: Tuesday , January 18, 2000

Please upgrade RiverPilot today.

Saved On: 10/7/99 4:35:39 PM

Description

The Group Notice is seen by users belonging to the specified group when they connect. The Notice is not seen by users after the expiration date has passed, although it is still displayed here.

Successfully updated Group Notice for Engineering

Click here to expand Global Area entries

Click this icon to open the Group Notice display

Click here to view the client update options

Choose a group

Choose a Date

Write your notice here

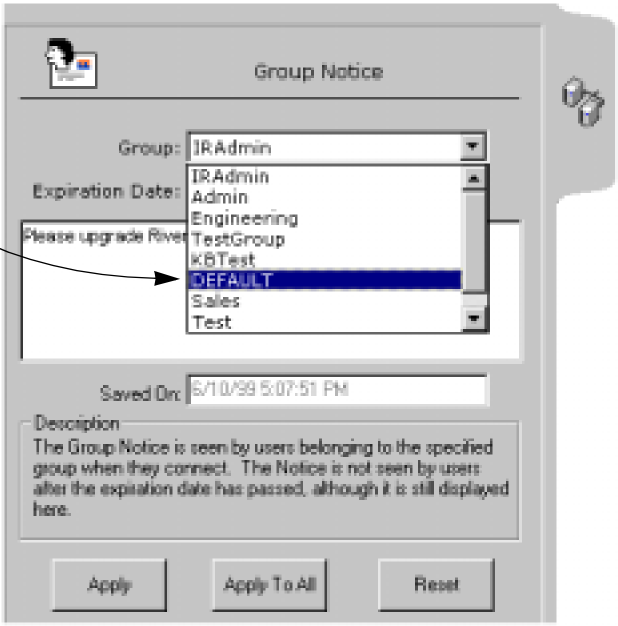
A message indicating Notice status displays here

Figure 82 Group Notice Display

5 Click the arrow in the Group field and select a group.

The Group pull-down screen appears as shown in Figure 83.

Select the Group you want to notify



Group: IRAdmin

IRAdmin
Admin
Engineering
TestGroup
KBTest
DEFAULT
Sales
Test

Please upgrade River

Saved On: 6/10/99 5:07:51 PM

The Group Notice is seen by users belonging to the specified group when they connect. The Notice is not seen by users after the expiration date has passed, although it is still displayed here.

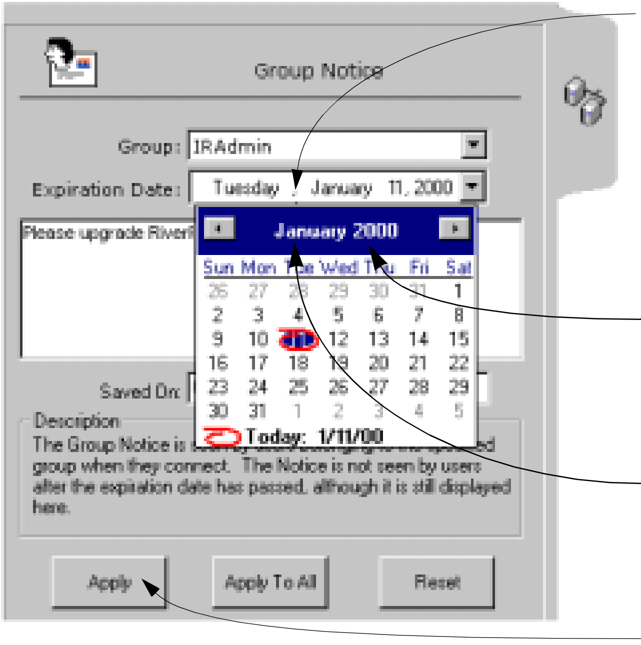
Figure 83 Group Notice Display Fields

6 Click the arrow in the Expiration Date field and set the date for this notice.

The Expiration Date pull-down screen appears as shown in Figure 84. Note that today's date is encircled in red ink for greater legibility. By clicking on the year or month, additional screens pop up to let you move the interval back or ahead incrementally.

NOTE

Notices expire on the date you set but they remain in the Group Notice text box until removed or a new notice is written.



Group Notice

Group: IRAdmin

Expiration Date: Tuesday , January 11, 2000

January 2000

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Today: 1/11/00

Please upgrade River

Saved On:

Description
The Group Notice is [illegible] ed group when they connect. The Notice is not seen by users after the expiration date has passed, although it is still displayed here.

Select the date you want to notify on

Move the year back or ahead by clicking on the year and opening a pop up screen here

Move the month back or ahead by clicking on the month and opening a pop up screen here

Click here to apply your notice to the selected group or all groups

Figure 84 Expiration Date Pull-Down Screen

7 Write your notice in the text box.

The message you write is limited to 256 characters. See Figure 82.

8 Click Apply to set the Notice for members of the selected Group or Apply to All to set the Notice for members of all groups.

If you made an error or want to change the selected date or group before applying the notice, edit the text and click Apply. See Figure 84. Clicking Reset retrieves the last screen saved.

7

Viewing Server Activity & Statistics

This chapter describes how to check activity on Aurorean Virtual Network systems by:

- Monitoring system activity, such as the messages exchanged between Aurorean Virtual Network servers and the RiverMaster.
- Viewing statistics information on active tunnel connections, including GRE packet and compression performance.
- Using SNMP to gather network statistics.

Monitoring System Activity

Using the Delivery service, Virtual Network systems and connected Aurorean Client Software clients exchange detailed messages with one another. RiverMaster captures this message activity as it occurs and displays the current messages in a viewer window. Messages are also stored in daily log files and can be later retrieved using an advanced message viewer.

Current Message Activity

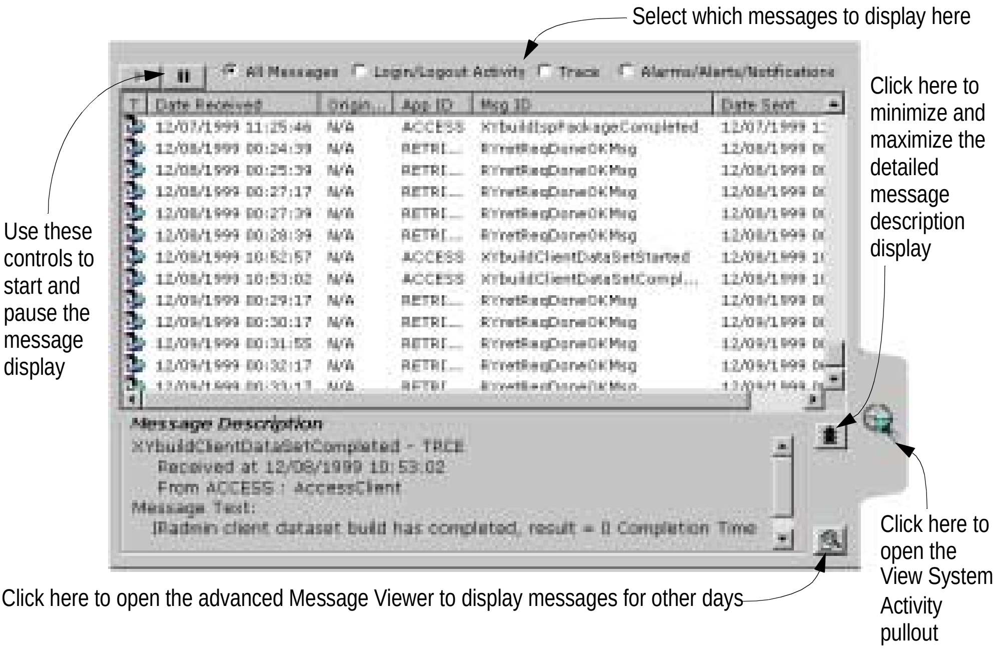
Using the RiverMaster message viewer, you can view all messages as they are sent or filter messages based on three categories:

- Remote user login and logout activity
- Trace messages generated by Enterasys services (such as the Authorization and Access services)
- Alarms, alerts, and problem notification messages produced by the Aurorean Policy Server or Aurorean Network Gateway.

To view message activity, perform the following steps:

1 Open the View System Activity pullout.

A sample message activity view is shown in Figure 85.


Select which messages to display here
Click here to minimize and maximize the detailed message description display
Use these controls to start and pause the message display
Click here to open the View System Activity pullout
Click here to open the advanced Message Viewer to display messages for other days
● All Messages
○ Login/Logout Activity
○ Trace
○ Alarms/Alerts/Notifications

T	Date Received	Origin...	App ID	Msg ID	Date Sent
	12/07/1999 11:25:46	N/A	ACCESS	XYbuildIspPackageCompleted	12/07/1999 1
	12/08/1999 00:24:39	N/A	RETRI...	RYretReqDoneOKMsg	12/08/1999 0
	12/08/1999 00:25:39	N/A	RETRI...	RYretReqDoneOKMsg	12/08/1999 0
	12/08/1999 00:27:17	N/A	RETRI...	RYretReqDoneOKMsg	12/08/1999 0
	12/08/1999 00:27:39	N/A	RETRI...	RYretReqDoneOKMsg	12/08/1999 0
	12/08/1999 00:28:39	N/A	RETRI...	RYretReqDoneOKMsg	12/08/1999 0
	12/08/1999 10:52:57	N/A	ACCESS	XYbuildClientDataSetStarted	12/08/1999 1
	12/08/1999 10:53:02	N/A	ACCESS	XYbuildClientDataSetCompl...	12/08/1999 1
	12/09/1999 00:29:17	N/A	RETRI...	RYretReqDoneOKMsg	12/09/1999 0
	12/09/1999 00:30:17	N/A	RETRI...	RYretReqDoneOKMsg	12/09/1999 0
	12/09/1999 00:31:55	N/A	RETRI...	RYretReqDoneOKMsg	12/09/1999 0
	12/09/1999 00:32:17	N/A	RETRI...	RYretReqDoneOKMsg	12/09/1999 0
	12/09/1999 00:33:17	N/A	RETRI...	RYretReqDoneOKMsg	12/09/1999 0

```
Message Description
XYbuildClientDataSetCompleted - TRCE
   Received at 12/08/1999 10:53:02
   From ACCESS : AccessClient
Message Text:
  IPadmin client dataset build has completed, result = 0 Completion Time
```

Figure 85 Message Activity WIndow

2 Select the types of messages you want to view by choosing one of the following:

– All Messages to view messages of all types generated by the APS and ANG, and Aurorean Client.

– **Login/Logout Activity** to limit the display to accounting/billing and authorization messages produced when remote clients log in and out.

– **Trace** to examine activity trace messages that contain details on tunnel protocol negotiation and remote client session reports sent in by Aurorean software.

– **Alarms/Alerts/Notifications** to check for alarm, alert, and problem notification messages that indicate problems at the Aurorean Network Gateway or Aurorean Policy Server or a remote client.

3 Use the play and pause buttons in the upper left corner to start and pause the message display.

During peak periods of activity, messages may scroll at a high rate. To pause the display to allow you to select a particular message to examine in detail, click the pause button. When the display is paused, the number of messages waiting to be shown appears in parentheses above the button. For example, if RiverMaster received five messages since you paused the display, (5) appears above the button.

Table 9 System Activity Display

Heading	Meaning
T	Message type; possible values are: 🔑 Authorization message resulting from a remote client's attempt to authenticate. Accounting and billing message indicating a remote client logging into or out of the VPN. Problem notification message signaling a connection problem at the Aurorean Network Gateway or the remote client. Activity trace message providing details on tunnel protocol negotiation and showing remote client session reports sent in by Aurorean Client software. ❌ Message from the Tunnel or Aurorean Policy Server indicating an alarm condition has occurred such as a server reboot or El Gamal key pair reissuance.
Date Received	The time and date RiverMaster received the message (based on the RiverMaster PC's clock).
Originator	The source of the message. Messages originating from the Tunnel or Aurorean Policy Server display the originator as "N/A." If the message was generated by Aurorean Client software, the remote client's user name appears in this column.

Table 9 System Activity Display (Continued)

Heading	Meaning
App ID	The IR service or software component that generated the message; possible values include: •*ACCESS* for messages from the Aurorean Policy Server. •*ADMIN* for messages generated by the IR Admin service. •*AUTH* for messages produced by the IR Authorization service. •*CLIENT* for messages produced by Aurorean Client software and sent over the tunnel. •*NOTIFICATION* for messages by the IR Notification service. •*OVERLORD* for messages sent by the IR Overlord Service. •*TUNNEL* for messages generated by the Aurorean Network Gateway.
Msg ID	Message ID that is unique for each message; refer to Table 10 on page 161 for a list of some message IDs.
Date Sent	The time and date the originator sent the message (based on the originating server or remote PC's clock).

4 To view a detailed description of a particular message, highlight the message in the display and examine the contents of the Message Description area.

Use the scroll bar in this area to view the entire description, or click the maximize button to expand the area. A sampling of messages that appear in this area are listed in alphabetical order by Message ID in Table 10.

NOTE

The Message Description area displays information for up to 2000 messages. After that threshold is reached, no information for highlighted messages is displayed in the Message Description area. You can still view the contents of a particular message by utilizing the Advanced Viewer and setting the search criteria to "zoom in" on the message. The results will display in the Message Viewer. Refer to "Advanced Message Viewer" on page 164 for details.

Table 10 System Activity Messages

Message ID	Message Type	Detailed Description
AAClientAuth	Authentication Authorization	The Client needs to be authorized
AAchallenge	Authentication Authorization	Challenge a user
AANewElgamalKey	Authentication Alarm	A new El Gamal key pair was generated; connections down until clients get new key
AAresponse	Authentication Authorization	Authentication service response
ADNameChange	Authentication Debug Trace	User *old name* is being authenticated as *new name*
AMInvalidElgamalKeys	Authentication Alarm	Invalid El Gamal keys detected
ANAuthFailed	Authentication Problem Notification	User *NAME* failed authentication *CODE*
ANBadDomain	Authentication Problem Notification	User *NAME* issued an invalid domain name
APAuthorization Trace	Authorization Activity Trace	Authentication service started
AYAuthSucceeded	Authentication Activity Trace	User *NAME* authenticated successfully
CBCconnStart	Client Accounting & Billing	*SESSION_ID*: User *NAME* connected
CBCconnStop	Client Accounting & Billing	*SESSION_ID*: User *NAME* disconnected.
CDRxTrace	Client Activity Trace	Rx: *PRESCRIBER_MESSAGE*
CNRxNotify	Client Problem Notification	Rx: *PRESCRIBER_MESSAGE*
CPCallhomeProblem	Client Problem Notification	Client problem reported

Table 10 System Activity Messages (Continued)

Message ID	Message Type	Detailed Description
CPCallhomeTrace	Client Problem Activity Trace	Client trace completed
GAauthenticate	General Authorization	Authenticate a User
GAquery	General Authorization	Query a user
GASet	General Authorization	Set user data
LMlowDiskSpaceMsg	Log Service Alarm	Free disk space has fallen below 85%
MAconfig	Admin Authorization	Configure authentication service
MBUserLoggedIn	Admin Accounting & Billing	Administrator *NAME* logged in
MBUserLoggedOut	Admin Accounting & Billing	Administrator *NAME* logged out
MMolordRebooting	Admin Alarm	Overlord service now rebooting, IR Authentication failed
MMolordRestartingProc Msg	Admin Alarm	Authentication stopped and restarted
MMolordRestarProc FailedMsg	Admin Alarm	Authentication stopped and restart failed
MMolordUpOK	Admin Alarm	Overlord service now running after the server rebooted
MNGenericProblem Msg	Admin Problem Notification	Generic problem/notification message: *TEXT*
MNntfyConfigRtrvFailed	Admin Problem Notification	Notification service: Could not retrieve configuration information
MNntfyMsgNotSent	Admin Problem Notification	Notification service: Notify message not transmitted
MNntfyNoSMTPsvrs	Admin Problem Notification	Notification service: No SMTP server configured
MYGenericTraceMsg	Admin Activity Trace	Generic activity/trace message: *TEXT*

Table 10 System Activity Messages (Continued)

Message ID	Message Type	Detailed Description
RYretReqDoneOKMsg	Retrieval Service Activity Trace	Statistics derived from completing request
TBUserLoggedIn	Tunnel Accounting & Billing	User *DOMAIN\USERNAME* logged in
TBUserLoggedOut	Tunnel Accounting & Billing	User *DOMAIN\USERNAME* logged out
TNDisconnect	Tunnel Problem Notification	Tunnel disconnected
TNAuthFailure	Tunnel Problem Notification	Authorization Failed for User *NAME*
TNTunnelProblem	Tunnel Problem Notification	*PROBLEM_MESSAGE*, Call ID = *TUNNEL_ID*
TNTunnelStop	Tunnel Problem Notification	Tunnel ID *ID#* stopped at *TIME*
TYConfiguration UpdateNfy	Tunnel Activity Trace	Tunnel service has updated its configuration with a result code
TYTunnelSvcStart Success	Tunnel Activity Trace	Tunnel service has started successfully
TYTunnelTrace	Tunnel Activity Trace	*TRACE_MESSAGE*, Call ID = *TUNNEL_ID*
XYBuildClientData SetCompleted	Access Activity Trace	Client dataset build completed with *RESULT* at *STOPDATE*
XYBuildClientData SetStarted	Access Activity Trace	Client dataset build began at *STARTDATE*
XYBuildIspPackage Completed	Access Activity Trace	ISP package build ended with *RESULT* at *STOPDATE*
XYBuildIspPackage Started	Access Activity Trace	ISP package build began at *STARTDATE*
XYClientSyncComplete	Access Activity Trace	Client synchronization completed for user

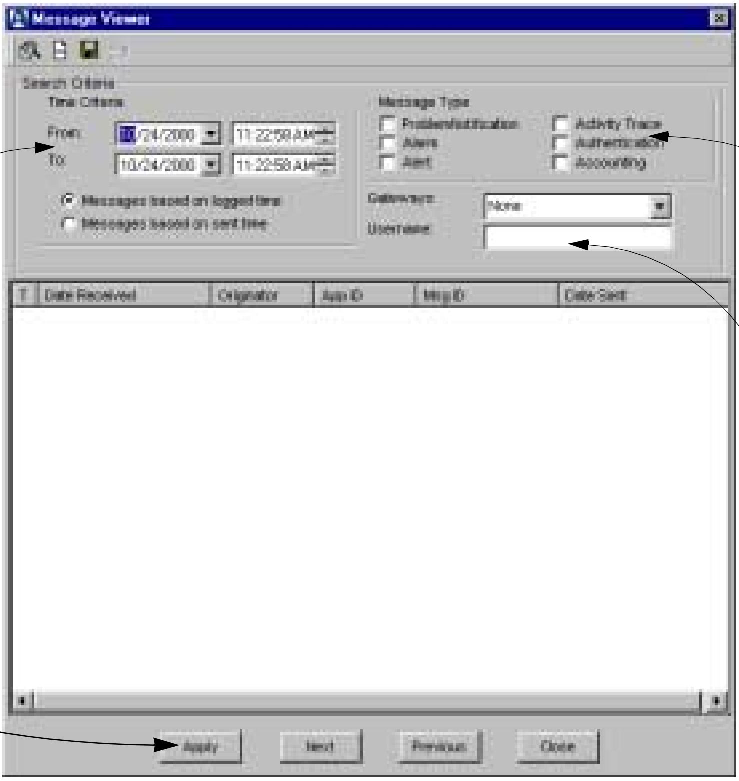
Advanced Message Viewer

While the standard message viewer displays current message activity, the advanced message viewer allows you to access messages that were sent on previous days or locate current messages buried in a large output of generated messages. Using the advanced message viewer, you can specify a period of time (for example, the previous week) and set message filter options for various types of messages. Based on this criteria, RiverMaster sends a query to the Aurorean Policy Server. Messages that match the criteria are extracted from log files and displayed in a separate message viewer window. After the query results are displayed, you can sort and print detailed descriptions for each message.

To open the advanced message viewer, perform these two steps:

1. Open the View System Activity pullout.
2. Click the Advanced Message Viewer button located at the bottom right corner of the pullout.

   The Message Viewer window appears as shown in Figure 86. This figure illustrates the settings to retrieve all login and logout activity for a single user over a two-week period.



From: 10/24/2000 11:22:58 AM
To: 10/24/2000 11:22:58 AM

● Messages based on logged time
○ Messages based on sent time

□ Problem/Notification
□ Alarm
□ Alert
□ Activity Trace
□ Authentication
□ Accounting

Gateways: None
Username:

Use these fields to set the start and end range of the message trace

Select which messages to display using the checkboxes

To display messages for a single user, enter the user's name here

Click here to start retrieving messages from the Aurorean Policy Server

Figure 86 Advanced Message View Setup Example

3 Using the Time Criteria fields, specify the period of time to display messages.

Use the From and To fields to specify the start date/time and end date/time. The time can be based on when the messages were received and logged by the Aurorean Policy Server (according to its system clock) or by when the messages were sent (based on the originator's clock). For best performance, sort the messages based on logged time.

4 Using the Message Type check boxes, specify the types of messages you want to view.

Table 11 describes the six types of messages available. To view Aurorean Virtual Network server activity, select Problem Notification, Alarm, and / or Alert messages. To view activity for an individual Aurorean user, select Activity Trace, Authentication, and / or Accounting messages.

Table 11 Message Types

Message Type	**Explanation**
Problem Notification	Typically these messages indicate a remote client connection problem which Aurorean Client's Prescriber feature diagnosed and reported. These messages are generated by the APS or ANG, not Aurorean users.
Alarm	These messages are generated when an error count threshold has been crossed and an alarm condition is imminent. These messages are generated by the APS or ANG, not Aurorean users.
Alert	These messages notify you when a significant error occurs with a service running on a Aurorean Virtual Network system or a general problem that is preventing the server from operating normally. These messages are generated by the APS or ANG, not Aurorean users.
Activity Trace	These messages cover a wide range of Aurorean user activity, including successful authentications, VPN user name changes, and Prescriber session reports. If you select this type, you must enter a Aurorean user's name in the Username field.
Authentication	These messages provide a detailed trace of challenge and response activity during the authentication process. If you select this type, you must enter a Aurorean user's name in the Username field.
Accounting	These messages track the login and logout activity of individual Aurorean users, including statistical data reported by the Aurorean application, and other connection statistics such as the ISP name, POP phone number, and connection speed. If you select this type, you must enter a Aurorean user's name in the Username field.

5 Choose the server that you want to monitor from the Servers list.

This option allows you to select either the APS or ANG and only applies when you are viewing Problem Notification, Alarm, or Alert messages. If you are viewing the other message types, this field defaults to None. The None selection sets *no* filtering of messages, allowing *all* server activity to display.

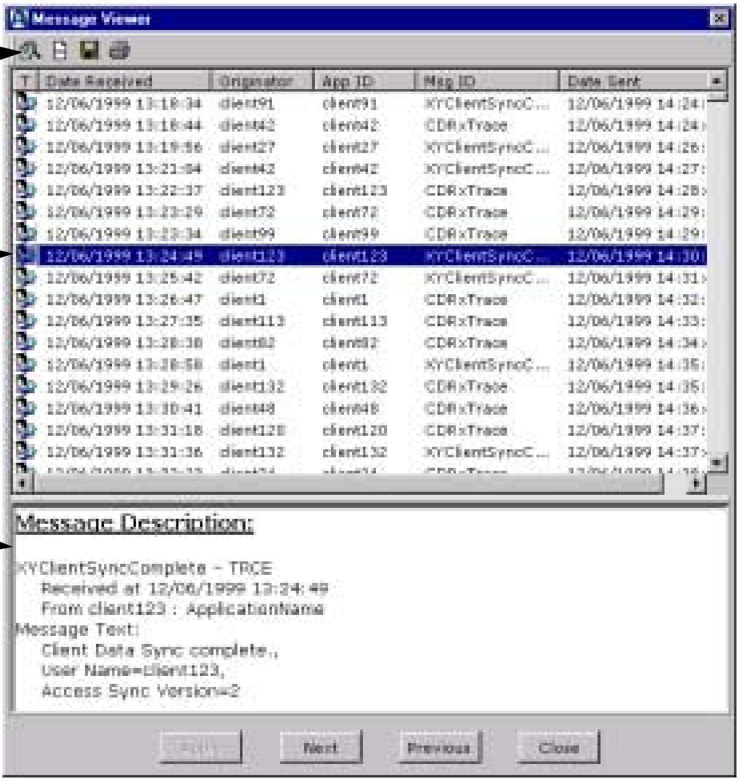
6 To view messages that originated from a specific user, enter the Aurorean Client's VPN user name in the Username field.

This option only applies when you are viewing Activity Trace, Authentication, or Accounting messages. The other message types relate to Aurorean Virtual Network system activity only.

7 Do one of the following:

- Click Apply to start retrieving messages from the Aurorean Policy Server.
- Click Close to close the Message Viewer window without retrieving messages.

When you click Apply, RiverMaster sends a query to the Aurorean Policy Server for the messages that fall within your parameters. This query may take several seconds; you can halt the query at any time by clicking Cancel. Figure 87 shows an example of the results from a message trace of all login and logout activity for a user over a two-week period.



Click here to start a new trace

Double-click on a message to view a detailed description

T	Date Received	Originator	App ID	Msg ID	Date Sent
	12/06/1999 13:18:34	client91	client91	XYClientSyncC...	12/06/1999 14:24:
	12/06/1999 13:18:44	client42	client42	CDRxTrace	12/06/1999 14:24:
	12/06/1999 13:19:56	client27	client27	XYClientSyncC...	12/06/1999 14:26:
	12/06/1999 13:21:04	client42	client42	XYClientSyncC...	12/06/1999 14:27:
	12/06/1999 13:22:37	client123	client123	CDRxTrace	12/06/1999 14:28:
	12/06/1999 13:23:29	client72	client72	CDRxTrace	12/06/1999 14:29:
	12/06/1999 13:23:34	client99	client99	CDRxTrace	12/06/1999 14:29:
	12/06/1999 13:24:49	client123	client123	XYClientSyncC...	12/06/1999 14:30:
	12/06/1999 13:25:42	client72	client72	XYClientSyncC...	12/06/1999 14:31:
	12/06/1999 13:26:47	client1	client1	CDRxTrace	12/06/1999 14:32:
	12/06/1999 13:27:35	client113	client113	CDRxTrace	12/06/1999 14:33:
	12/06/1999 13:28:38	client82	client82	CDRxTrace	12/06/1999 14:34:
	12/06/1999 13:28:58	client1	client1	XYClientSyncC...	12/06/1999 14:35:
	12/06/1999 13:29:26	client132	client132	CDRxTrace	12/06/1999 14:35:
	12/06/1999 13:30:41	client48	client48	CDRxTrace	12/06/1999 14:36:
	12/06/1999 13:31:18	client128	client120	CDRxTrace	12/06/1999 14:37:
	12/06/1999 13:31:36	client132	client132	XYClientSyncC...	12/06/1999 14:37:

Message Description:

```
XYClientSyncComplete - TRCE
   Received at 12/06/1999 13:24:49
   From client123 : ApplicationName
Message Text:
   Client Data Sync complete.,
   User Name=client123,
   Access Sync Version=2
```

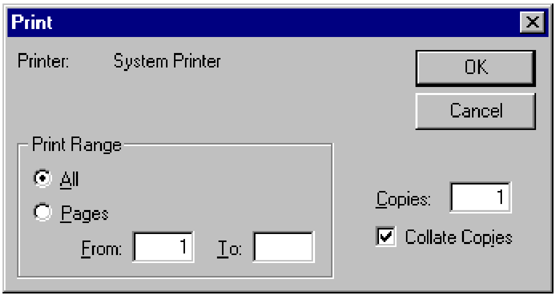
Figure 87 Advanced Message Viewer Results Example

8 To view a detailed description of a message, double-click on the message.

Figure 87 shows the details of a Connection Start message that reveals information on how the Aurorean Client connected a client named Paul.

9 Do one of the following:

- To retrieve another set of messages, click the Search Messages icon and return to Step 3.
- To open or close the window pane that displays detailed description for each message, click the Enable Preview Pane icon. Toggling this button enables and disables the Print icon.
- To save the query result to a file, click the Save Messages As icon. The results can be saved as a text-only `.OUT` file or formatted as a Aurorean Virtual Network report. For more information on report formats, refer to Chapter 8.
- To print the query results, click the Print icon. A Print window appears as shown in Figure 88; set the printing options and click OK.



Printer: System Printer

Print Range
● All
○ Pages
From: 1 To:

Copies: 1
☑ Collate Copies

Figure 88 Printing Messages

NOTE

If you do not have at least one printer driver installed on your computer, the printer button is disabled. To install a printer, follow the instructions provided in Windows on-line Help.

RiverMaster Options

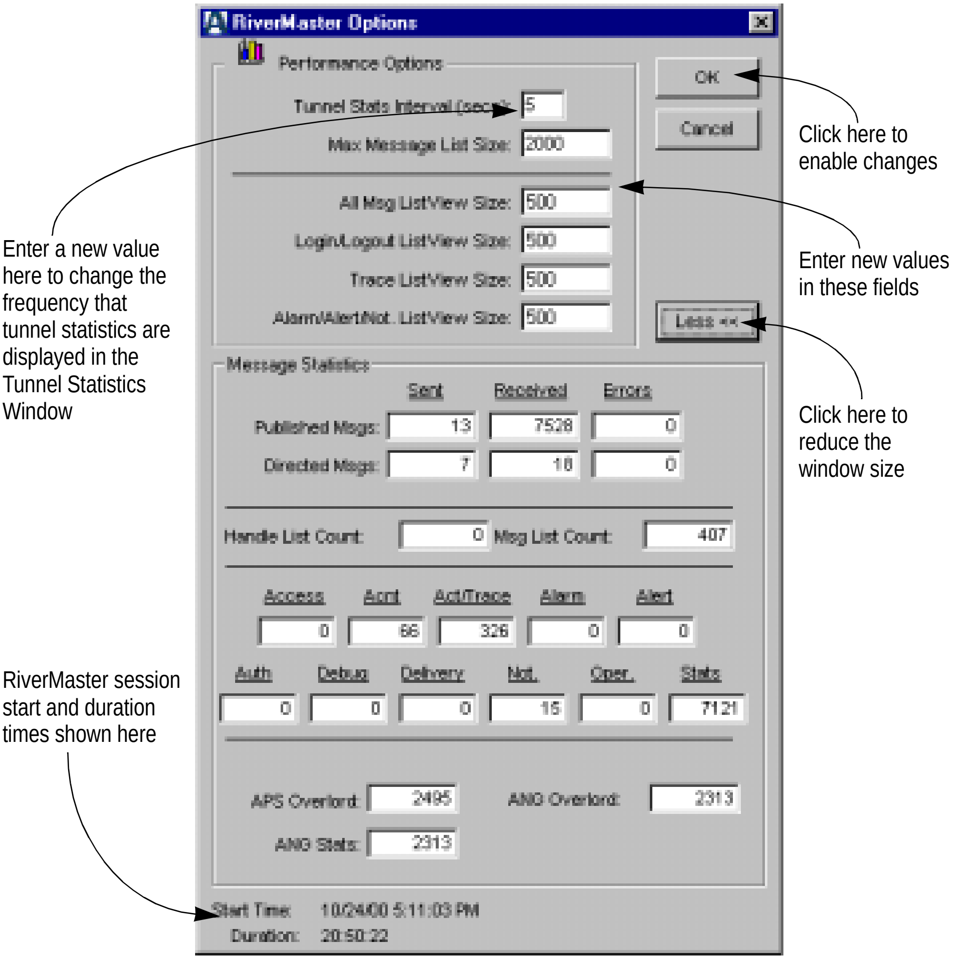
The RiverMaster Options button performs the following functions:

- Controls the number of messages and the frequency they are shown in the Message Viewer. Messages are displayed in the Tunnel Statistics window every 5 seconds (default) and are rolled over after reaching the default maximum of 2000 messages. All four ListView sizes are defaulted at 500 messages.
- When the window is enlarged, it displays RiverMaster session and message data. The start and duration of the current session is displayed at the bottom of the window. Message Statistics are also displayed but only for informational purposes to be interpreted with the help of Enterasys Customer Support personnel.

To use RiverMaster Options, perform the following steps:

1 At the RiverMaster main interface, click the RiverMaster Options button above the service status screen.

The RiverMaster Options window displays as shown in Figure 89.



Performance Options

Tunnel Stats Interval (secs): 5
Max Message List Size: 2000
All Msg ListView Size: 500
Login/Logout ListView Size: 500
Trace ListView Size: 500
Alarm/Alert/Not. ListView Size: 500

Message Statistics

	Sent	Received	Errors
Published Msgs:	13	7528	0
Directed Msgs:	7	18	0

Handle List Count: 0 Msg List Count: 407

Access	Acnt	Act/Trace	Alarm	Alert
0	66	326	0	0

Auth	Debug	Delivery	Not.	Oper.	Stats
0	0	0	16	0	7121

APS Overlord: 2495 ANG Overlord: 2313
ANG Stats: 2313

Start Time: 10/24/00 5:11:03 PM
Duration: 20:50:22

Enter a new value here to change the frequency that tunnel statistics are displayed in the Tunnel Statistics Window

RiverMaster session start and duration times shown here

Click here to enable changes

Enter new values in these fields

Click here to reduce the window size

Figure 89 RiverMaster Options Window

2 In the Performance Options area, enter a value for any message interval.

The Tunnel Stats Interval is the frequency with which user tunnel statistics are recorded in the Tunnel Statistics Window (refer to “Viewing Tunnel Activity” on page 173 for more information).

3 If you wish to change the Max Message List Size or any of the four ListView sizes, enter a value in the provided field.

Size values refer to the maximum number of messages displayed in the Message Viewer according to the message type selected. Message Types include All Messages, Login / Logout, Trace, and Alarm / Alert / Notices.

4 Click More to display Message Statistics, the time when this RiverMaster session began and its duration.

The Published and Directed messages, and Handle and Message List counters are internal to RiverMaster operations. Various IR Service and other messages reflect similar internal counters.

5 Click OK to save Performance Option changes or Cancel to exit the window without changing the values.

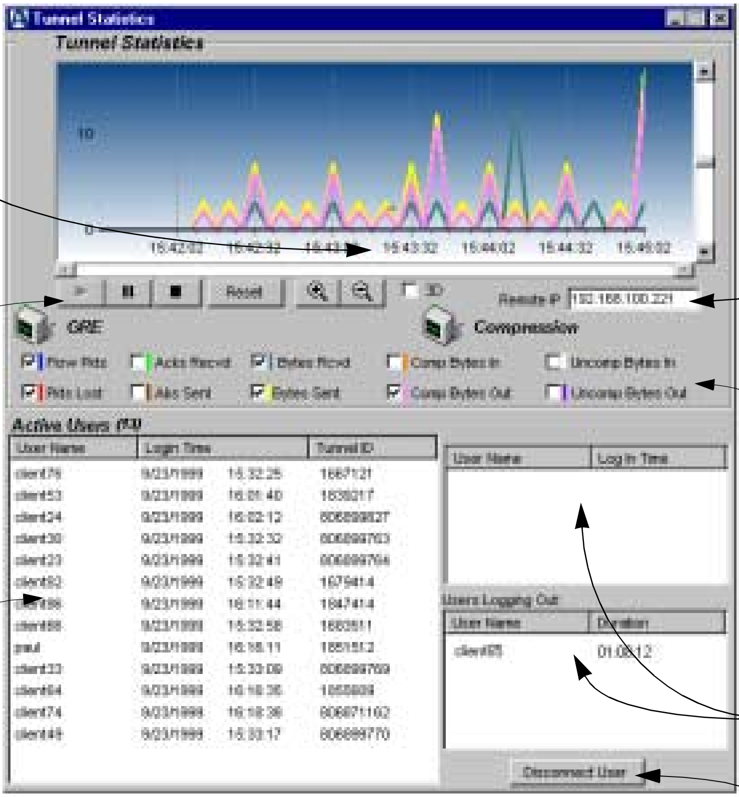
Viewing Tunnel Activity

The Tunnel Statistics window displays counters in graphic and column form. The graphical window can be configured to display any Generic Routing Encapsulation (GRE) or compression counters you select in the available checkboxes. The Active Users boxes show the User Name, Login Time and Tunnel ID for users logged in, and log in or session time for users who are currently logging in or out.

To view data for a user currently tunneled into the network, do the following:

1 On the main RiverMaster interface, click the Aurorean Network Gateway Details button.

A Tunnel Statistics window appears similar to Figure 90.



☐ 3D

Remote IP 192.168.100.221

☑ Flow Pkts ☐ Acks Recvd ☑ Bytes Rcvd ☐ Comp Bytes In ☐ Uncomp Bytes In
☑ Pkts Lost ☐ Aks Sent ☑ Bytes Sent ☑ Comp Bytes Out ☐ Uncomp Bytes Out

Active Users (13)

User Name	Login Time		Tunnel ID
client76	9/23/1999	15:32:25	1667121
client53	9/23/1999	16:01:40	1636217
client24	9/23/1999	16:02:12	806899327
client30	9/23/1999	15:32:32	806899763
client23	9/23/1999	15:32:41	806899764
client93	9/23/1999	15:32:49	1679414
client96	9/23/1999	16:11:44	1647414
client88	9/23/1999	15:32:58	1683511
paul	9/23/1999	16:16:11	1685152
client33	9/23/1999	15:33:09	806899769
client64	9/23/1999	16:16:35	1055839
client74	9/23/1999	16:18:39	806871162
client49	9/23/1999	15:33:17	806899770

User Name	Log In Time

Users Logging Out

User Name	Duration
client85	01:08:12

Control the frequency that user tunnel data are displayed by adjusting the Tunnel Stats Interval with the RiverMaster Options button

Use these buttons to control the tunnel statistics graph

Connected users appear here

IP address derived from the virtual subnet or static address given to the client for the duration of the connection

Select the statistics you want to graph here

Users in the process of logging in or out appear here

Disconnect active user here

Figure 90 Tunnel Statistics Window

2 From the Active Users list, click on a user name.

3 Using the GRE and Compression checkboxes, choose the types of statistics you want to graph for the selected user.

Table 12 describes the types of statistics you can choose.

Table 12 Protocol Statistics

Value		**Meaning**	**Trends to Look For...**
GRE (Generic Routing Encapsulation)	Flow Pkts	The number of GRE packets dropped by the Aurorean Network Gateway due to flow control and full receive buffers.	This value usually indicates congestion at the Aurorean Network Gateway caused by a large number of users logged in and/or a high volume of data being transferred. Sudden spikes in this graph occur when the Aurorean Network Gateway is unable to keep pace with incoming tunnel packets.
	Pkts Lost	The number of GRE packets lost by the Aurorean Network Gateway.	This value indicates checksum failures, corrupted packet headers, or flow control problems (the Flow Pkts count is included in this value). Sudden spikes in this graph occur when the Aurorean Network Gateway is unable to keep pace with incoming tunnel packets.
	Acks Recvd	The number of GRE acknowledgment packets received by the Aurorean Network Gateway.	These values result from overhead traffic between the Aurorean Network Gateway and the remote client (packets which did not contain actual user data). Sudden spikes usually occur when a connection begins as the Aurorean Network Gateway and remote client negotiate authentication, encryption, and compression options to use on the connection.
	Acks Sent	The number of GRE acknowledgment packets sent to the remote client.	

Table 12 Protocol Statistics (Continued)

Value		**Meaning**	**Trends to Look For...**
GRE (Generic Routing Encapsulation)	Bytes Rcvd	The total number of GRE bytes received by the Aurorean Network Gateway over the tunnel.	These values describe the actual payload data (without packet headers) sent and received over the tunnel. Sudden spikes usually occur when a remote client starts to download or upload a large file.
	Bytes Sent	The total number of GRE bytes sent to the remote client over the tunnel.	
Compression	Comp Bytes In	The total number of compressed bytes received by the Aurorean Network Gateway over the tunnel.	The values show the level of activity on the tunnel and indicate how effective compression is on this connection. Very low numbers indicate that compression was not negotiated for this connection or that the data passing over the tunnel is not compressible.
	Comp Bytes Out	The total number of compressed bytes sent to the remote user over the tunnel.	
	Uncomp Bytes In	The total number of uncompressed bytes received by the Aurorean Network Gateway over the tunnel.	
	Uncomp Bytes Out	The total number of uncompressed bytes sent to the remote user over the tunnel.	

4 Using the controls shown in Figure 91, control the graph display as follows:

– To start and stop the display, use the Play and Stop buttons.

– To temporarily freeze the display to examine activity at a specific point in time, use the Pause button.

– To clear the display and restart the graph, use the Reset button.

– To adjust the scale to closely examine an individual graph or pull back to view all graphs, use the Zoom In and Zoom Out buttons.

– To view the graphs as 3-dimensional objects rather than simply 2-dimensional lines, place a check next to 3D.

NOTE

You can disconnect an active user by selecting a user from the Active Users list and clicking the Disconnect User button, as shown in Figure 90.

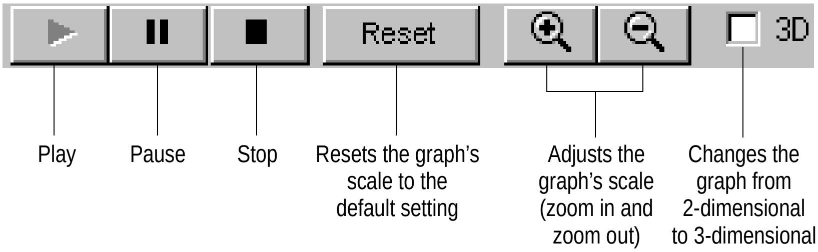

Reset
3D
Play
Pause
Stop
Resets the graph's scale to the default setting
Adjusts the graph's scale (zoom in and zoom out)
Changes the graph from 2-dimensional to 3-dimensional

Figure 91 Protocol Statistics Display Controls

To gain additional details about the user (such as how the user was authenticated), use the System Activity pullout as described in “Monitoring System Activity” on page 157.

Using SNMP to Gather Statistics

Aurorean Virtual Network software supports two private MIBs as well as standard SNMP MIBs for statistical analysis by any common network management tool. The proprietary MIBs, `etsys-aps-MIB` and `etsys-ang-MIB`, are stored on the Aurorean System Software CD ROM and are read-only.

8

Generating Reports

This chapter describes the contents of the customized reports available from RiverMaster and describes how to download, view, export and print these reports.

Report Contents

Each initial (Preview) Aurorean report shows all activity for the selected period. Subsequent, “drill-down” displays categorize activity into user-specific data for Accounting and Client reports. Additionally, the Network Gateway Report displays a bar graph. The following reports are available:

- Server Anomaly Report
- Network Gateway Report
- Client Anomaly Report
- Client Report
- Accounting Report

Server Anomaly Report

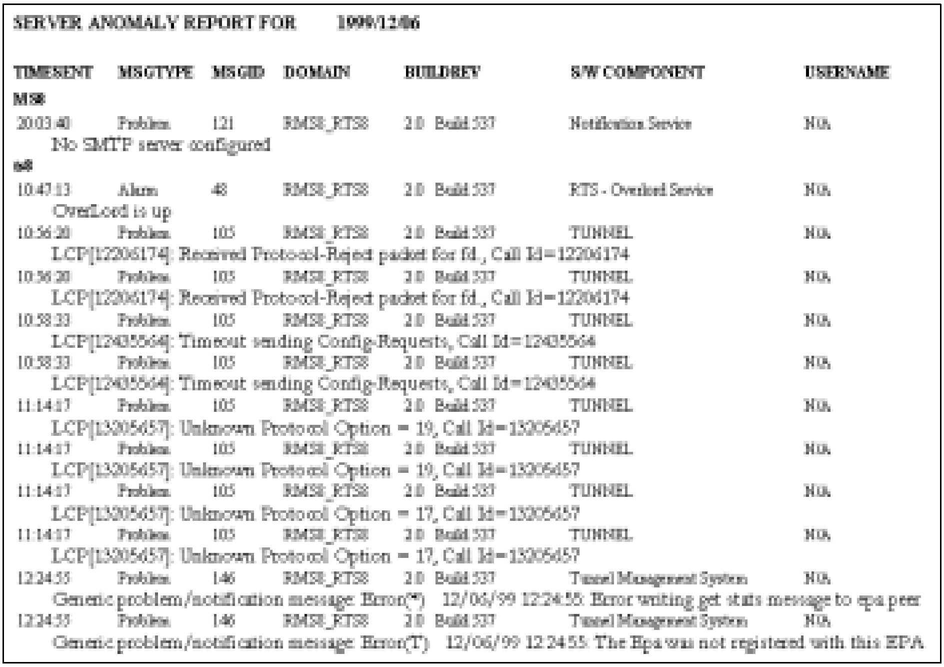
This report lists the alarm, alert, and problem notification messages produced by the Aurorean Policy Server and Aurorean Network Gateway for that period. The messages are ordered by server name and then listed according to the time they were received.

Table 13 lists the column headings and values that appear in a Server Anomaly Report. A text area under each message also provides a detailed description of the cause of the condition.

Table 13 Server Anomaly Report Values

Heading	**Explanation**
TIMESENT	Time the message was sent (according to the server's clock).
MSGTYPE	Category of the anomaly message; possible values are: *Alarms* for server alarm conditions. *Alerts* for alert conditions that may lead to an alarm state. *Problem* for problem notification messages.
MSGID	An ID number useful for Enterasys Networks Customer Support personnel to isolate the problem.
DOMAIN	The Aurorean Policy Server Domain name assigned to servers within this Aurorean Virtual Network.
BUILDREV	Version of Aurorean system software installed and running on the server in the format: *Release# Build#* where *Release#* indicates the functionality release (such as 3.0) and *Build#* indicates an Enterasys Networks internal software version number.
S/W COMPONENT	Software component that reported the anomaly. Possible values include: Authorize Notification Service Aurorean Client Software APS - Log Service APS - Overlord Service ANG - Overlord Service TUNNEL
USERNAME	Name of the remote user experiencing the problem. If the problem was not caused by Aurorean Client Software connection, this field contains "N/A".

Figure 92 displays a typical Server Anomaly Report.



```
SERVER ANOMALY REPORT FOR        1999/12/06

TIMESENT     MSGTYPE    MSGID   DOMAIN        BUILDREV          S/W COMPONENT              USERNAME
MS8
 20:03:40    Problem    121     RMS8_RTS8     2.0  Build 537    Notification Service       N/A
     No SMTP server configured
ts8
 10:47:13    Alarm      48      RMS8_RTS8     2.0  Build 537    RTS - Overload Service     N/A
     OverLoad is up
 10:56:20    Problem    105     RMS8_RTS8     2.0  Build 537    TUNNEL                     N/A
     LCP[12206174]: Received Protocol-Reject packet for fd., Call Id=12206174
 10:56:20    Problem    105     RMS8_RTS8     2.0  Build 537    TUNNEL                     N/A
     LCP[12206174]: Received Protocol-Reject packet for fd., Call Id=12206174
 10:58:33    Problem    105     RMS8_RTS8     2.0  Build 537    TUNNEL                     N/A
     LCP[12435564]: Timeout sending Config-Requests, Call Id=12435564
 10:58:33    Problem    105     RMS8_RTS8     2.0  Build 537    TUNNEL                     N/A
     LCP[12435564]: Timeout sending Config-Requests, Call Id=12435564
 11:14:17    Problem    105     RMS8_RTS8     2.0  Build 537    TUNNEL                     N/A
     LCP[13205657]: Unknown Protocol Option = 19, Call Id=13205657
 11:14:17    Problem    105     RMS8_RTS8     2.0  Build 537    TUNNEL                     N/A
     LCP[13205657]: Unknown Protocol Option = 19, Call Id=13205657
 11:14:17    Problem    105     RMS8_RTS8     2.0  Build 537    TUNNEL                     N/A
     LCP[13205657]: Unknown Protocol Option = 17, Call Id=13205657
 11:14:17    Problem    105     RMS8_RTS8     2.0  Build 537    TUNNEL                     N/A
     LCP[13205657]: Unknown Protocol Option = 17, Call Id=13205657
 12:24:55    Problem    146     RMS8_RTS8     2.0  Build 537    Tunnel Management System   N/A
     Generic problem/notification message: Error(*)   12/06/99 12:24:55: Error writing get stats message to epa peer
 12:24:55    Problem    146     RMS8_RTS8     2.0  Build 537    Tunnel Management System   N/A
     Generic problem/notification message: Error(T)   12/06/99 12:24:55: The Epa was not registered with this EPA
```

Figure 92 Server Anomaly Report

Network Gateway Report

This report reveals the Aurorean Network Gateway's throughput performance by showing byte / packet traffic over all tunnels connected to the Aurorean Network Gateway. Separate performance statistics are shown for tunnels using GRE (PPTP) and IPSec protocols. These statistics are reported for each 1-hour period.

Table 14 lists the column headings and values that appear in the Network Gateway Report.

Table 14 Network Gateway Report Values

Heading	Explanation
Max Tunnels	Total number of remote clients that connected during the one-hour period.
Bytes IN	Number of bytes received over all tunnels by the Aurorean Network Gateway during the one-hour period. Bytes are shown in terms of total counts (in 1000 byte increments) and bytes per second throughput.
Bytes OUT	Number of bytes transmitted over all tunnels from the Aurorean Network Gateway during the one-hour period. Bytes are shown in terms of total counts (in 1000 byte increments) and bytes per second throughput.
Packets IN	Number of packets received over all tunnels by the Aurorean Network Gateway during the one-hour period. Packets are shown in terms of total counts and packets per second throughput.
Packets OUT	Total number of packets transmitted over all tunnels from the Aurorean Network Gateway during the one-hour period. Packets are shown in terms of total counts and packets per second throughput.

The first page of the Network Gateway Report is a bar graph, as shown in Figure 93, displaying the peak number of IPSec and GRE tunnels (number of remote clients) generated hourly for the selected period. The second and subsequent pages of the Network Gateway Report show the numerical information detailed in the preceding table and displayed in Figure 94.

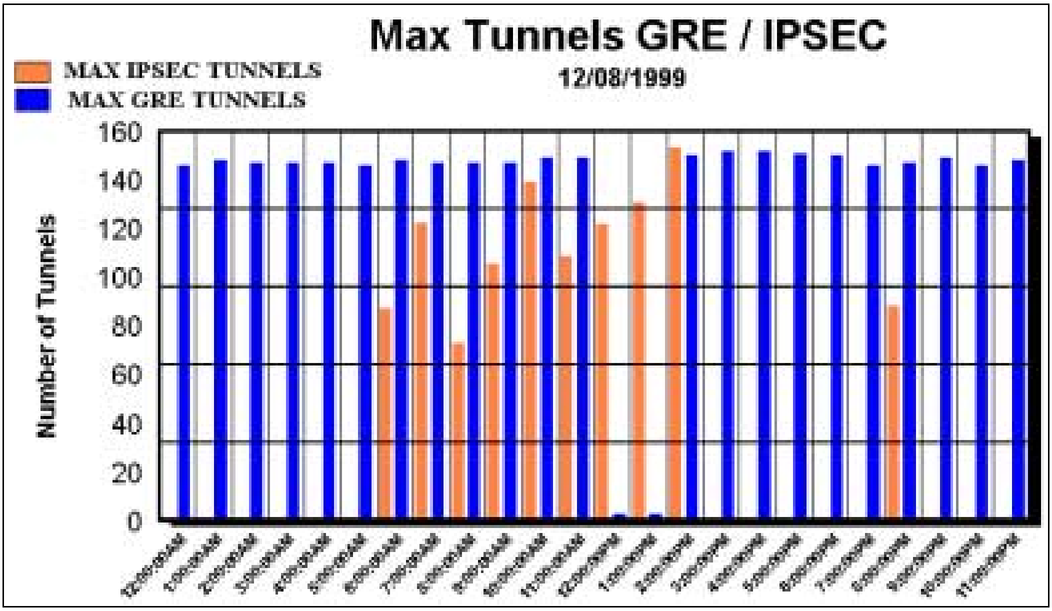
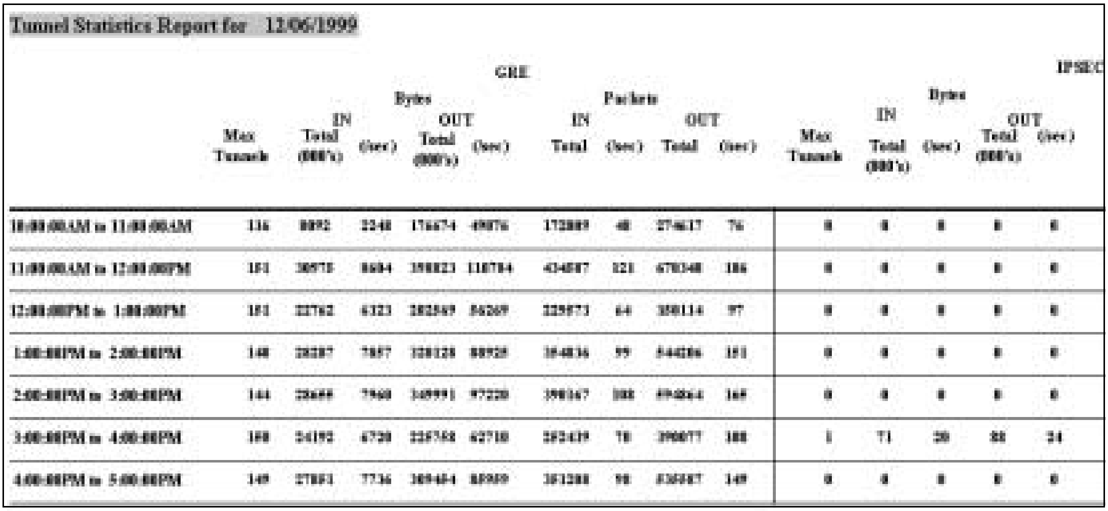


Figure 93 Max Tunnels GRE/IPSEC Display



Tunnel Statistics Report for 12/06/1999

	GRE									IPSEC				
		Bytes				Packets					Bytes			
		IN		OUT		IN		OUT			IN		OUT	
	Max Tunnels	Total (000's)	(sec)	Total (000's)	(sec)	Total	(sec)	Total	(sec)	Max Tunnels	Total (000's)	(sec)	Total (000's)	(sec)
10:00:00AM to 11:00:00AM	136	8092	2248	176674	49076	172889	48	274617	76	0	0	0	0	0
11:00:00AM to 12:00:00PM	151	30978	8604	398823	110784	434087	121	670348	186	0	0	0	0	0
12:00:00PM to 1:00:00PM	151	22762	6323	310569	86269	229973	64	350114	97	0	0	0	0	0
1:00:00PM to 2:00:00PM	148	28287	7857	320128	88928	354836	99	544286	151	0	0	0	0	0
2:00:00PM to 3:00:00PM	144	28659	7960	349991	97220	388167	108	594064	165	0	0	0	0	0
3:00:00PM to 4:00:00PM	160	24192	6720	225768	62710	282419	78	390077	108	1	71	20	88	24
4:00:00PM to 5:00:00PM	149	27851	7736	309464	85962	351288	98	536087	149	0	0	0	0	0

Figure 94 Network Gateway Report

Client Anomaly Report

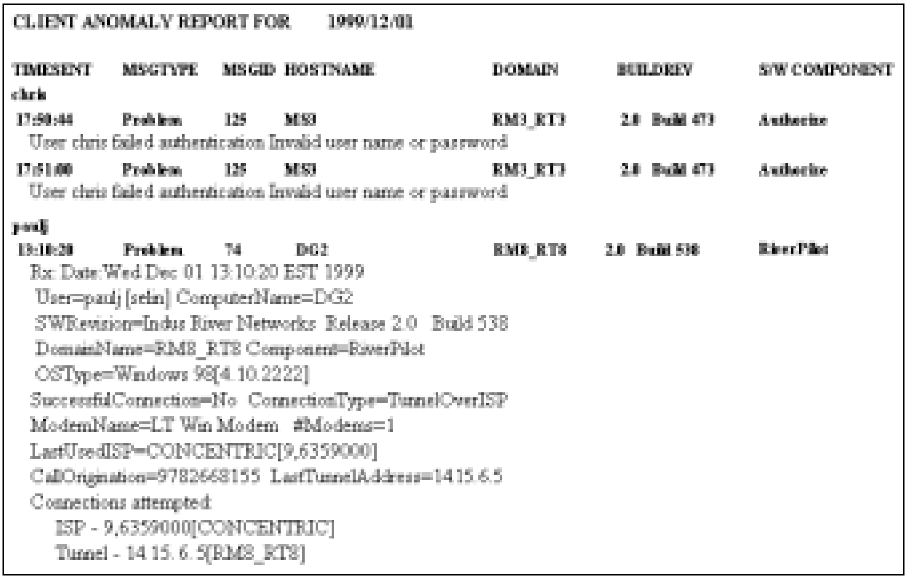
This report lists Aurorean Client Software connection problems such as authentication failures and other failed tunnel attempts. These events are sorted by the remote client's user name and then listed according to the time they were sent.

Table 15 lists the column headings and values that appear in a Client Anomaly Report. A text area under each message also provides a detailed description of the cause of the condition.

Table 15 Client Anomaly Report Values

Heading	Explanation
TIMESENT	The time the event occurred (according to the remote client PC's clock) in *Hour:Minute:Second* military format.
MSGTYPE	Category of the anomaly message; possible values are: *Alarms* for Aurorean Client Software alarm conditions. *Alerts* for alert conditions that may lead to an alarm state. *Problem* for problem notification messages.
MSGID	An ID number useful for Enterasys Networks Customer Support personnel to isolate the problem.
HOSTNAME	The computer name assigned to the remote client's computer.
DOMAIN	The APS Domain name given this Aurorean Virtual Network.
BUILDREV	Version of Aurorean Client Software installed and running on the remote client in the format: *Release# Build#* where *Release#* indicates the functionality release (e.g. 3.0) and *Build#* indicates an internal software version number.
S/W COMPONENT	Software component that reported the anomaly. Possible values include: Authorize Aurorean Client

Figure 95 displays a typical Client Anomaly Report.



```
CLIENT ANOMALY REPORT FOR      1999/12/01

TIMESENT      MSGTYPE    MSGID  HOSTNAME                 DOMAIN       BUILDREV         S/W COMPONENT
chris
 17:50:44     Problem    125    MS3                      RM3_RT3       2.0  Build 473  Authorize
   User chris failed authentication Invalid user name or password
 17:51:00     Problem    125    MS3                      RM3_RT3       2.0  Build 473  Authorize
   User chris failed authentication Invalid user name or password

paulj
 13:10:20     Problem    74      DG2                     RM8_RT8      2.0  Build 538   RiverPilot
   Rx: Date:Wed Dec 01 13:10:20 EST 1999
    User=paulj [selin] ComputerName=DG2
    SWRevision=Indus River Networks  Release 2.0   Build 538
    DomainName=RM8_RT8 Component=RiverPilot
    OSType=Windows 98[4.10.2222]
   SuccessfulConnection=No  ConnectionType=TunnelOverISP
   ModemName=LT Win Modem   #Modems=1
   LastUsedISP=CONCENTRIC[9,6359000]
   CallOrigination=9782668155  LastTunnelAddress=14.15.6.5
   Connections attempted:
       ISP - 9,6359000[CONCENTRIC]
       Tunnel - 14.15. 6. 5[RM8_RT8]
```

Figure 95 Client Anomaly Report

In addition to the information listed in Table 15, an anomaly event may include a session report produced by Aurorean Client Software's Prescriber feature. This session report describes the remedies that Prescriber attempted to correct the problem; for more information on Prescriber and this session report, refer to the *Aurorean Client Software User's Guide*.

Client Report

This report lists all successful tunnel sessions into the Aurorean Network Gateway, and is useful for identifying each time a user connected during the selected period. Sessions are sorted first by user name then ISP; if the user logged into the Aurorean Network Gateway more than once that day, the sessions are listed in the order they occurred. For each user, the report calculates the average connection time and the total amount of time connected, as well as totals the byte and packet counts for all sessions.

The report also indicates the ISP that was used for each session (or shows "Pre-existing Connection" for non-dialed LAN link or cable modem connections). In addition to the data described in the following table, throughput averages and sums, and login session totals and average intervals are reported for each user and ISP. This report also offers a drill-down view in a subsequent display.

Table 16 lists the column headings and values that appear in a Client Report.

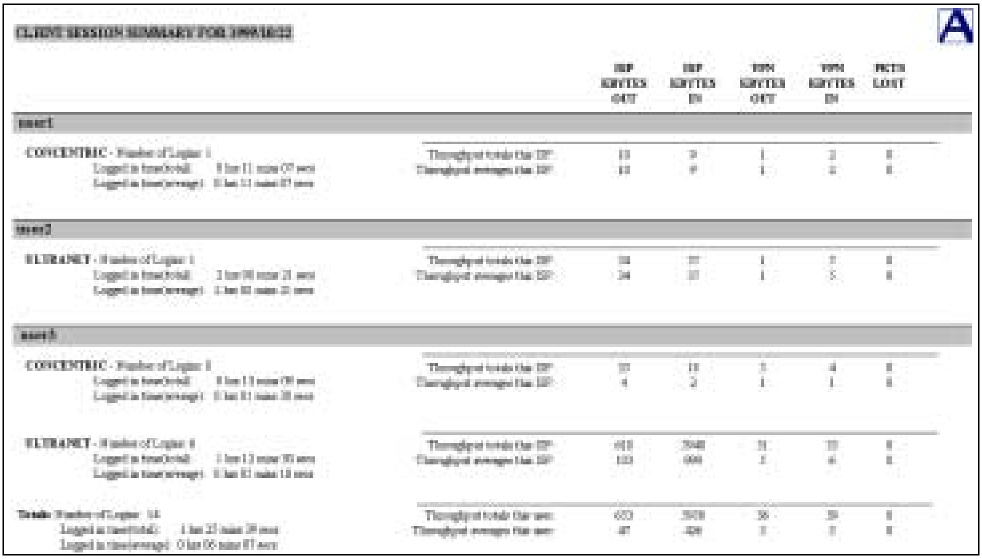
Table 16 Client Session Report Values

Heading	Explanation
TIME IN	Time the tunnel session started (according to the remote client PC's clock) in the format: *Year/Month/Day Time* where *Time* is shown in military time.
TIME OUT	Time the tunnel session ended (according to the remote client PC's clock) in the format: *Year/Month/Day Time* where *Time* is shown in military time.
HOST NAME	The computer name assigned to the remote client's computer.
PROTOCOL	The security protocol used on the tunnel: *IPSEC-HTTPS* for an ANG that negotiated the IPSec and HTTPS protocols. *PPTP* for an ANG that negotiated thePPTP protocol.
POP PHONE #	Phone number of the POP that Aurorean Client dialed into ("N/A" for clients using an existing Internet connection such as a cable modem or LAN link).
FROM PHONE #	The remote client's location phone number (the phone number entered on the Aurorean Client From pullout).
CONN TYPE	Type of connection(s) used by the remote client to reach the Aurorean Network Gateway. Possible values include: *Both* for sessions involving a dial-up connection into a POP and then a tunnel. *Tunnel* for tunnels that used an existing Internet connection (LAN link or cable modem).

Table 16 Client Session Report Values

Heading	Explanation
CONN SPEED	Connect speed of the analog modem in bits per second (“N/A” for clients using an existing Internet connection such as a cable modem or LAN link).
ISP KBYTES OUT	Total bytes of data sent from the Aurorean user to the ISP POP during the session.
ISP KBYTES IN	Total bytes of data sent from the ISP POP to the Aurorean user during the session.
VPN KBYTES OUT	Total bytes of data sent end-to-end over the tunnel from the Aurorean user to the corporate network during the session.
VPN KBYTES IN	Total bytes of data sent end-to-end over the tunnel from the corporate network to the Aurorean user during the session.
PKTS LOST	Number of packets dropped during the session due to flow control or checksum errors.
User # of logins	Number of logins by the specified user
Total time	Total interval of time the specified user was logged in
Average login time	Average session time of specified user

Figure 96 displays a typical Client Session Summary Report.

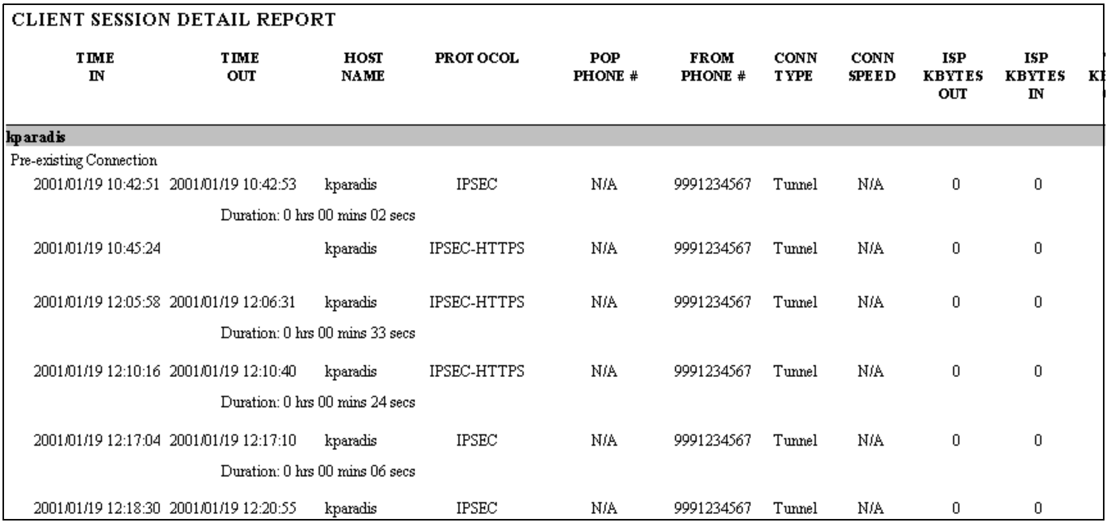


CLIENT SESSION SUMMARY FOR 1999/10/22

		ISP KBYTES OUT	ISP KBYTES IN	VPN KBYTES OUT	VPN KBYTES IN	PKTS LOST
user1						
CONCENTRIC - Number of Logins 1 Logged in time(total) 0 hrs 11 mins 07 secs Logged in time(average) 0 hrs 11 mins 07 secs	Throughput totals thru ISP Throughput averages thru ISP	13 13	9 9	1 1	2 2	0 0
user2						
ULTRANET - Number of Logins 1 Logged in time(total) 2 hrs 00 mins 21 secs Logged in time(average) 2 hrs 00 mins 21 secs	Throughput totals thru ISP Throughput averages thru ISP	24 24	37 37	1 1	5 5	0 0
user3						
CONCENTRIC - Number of Logins 8 Logged in time(total) 0 hrs 13 mins 09 secs Logged in time(average) 0 hrs 01 mins 38 secs	Throughput totals thru ISP Throughput averages thru ISP	37 4	13 2	5 1	4 1	0 0
ULTRANET - Number of Logins 5 Logged in time(total) 1 hrs 12 mins 30 secs Logged in time(average) 0 hrs 03 mins 13 secs	Throughput totals thru ISP Throughput averages thru ISP	613 123	3040 608	11 2	33 6	0 0
Totals: Number of Logins 14 Logged in time(total) 1 hrs 25 mins 39 secs Logged in time(average) 0 hrs 06 mins 07 secs	Throughput totals thru user Throughput averages thru user	653 47	3109 428	36 3	39 3	0 0

Figure 96 Client Session Summary Report

Double-clicking on the user name line above with the magnifier icon produces a drill-down view similar to Figure 97.



CLIENT SESSION DETAIL REPORT

TIME IN	TIME OUT	HOST NAME	PROTOCOL	POP PHONE #	FROM PHONE #	CONN TYPE	CONN SPEED	ISP KBYTES OUT	ISP KBYTES IN	KI
kparadis										
Pre-existing Connection										
2001/01/19 10:42:51	2001/01/19 10:42:53	kparadis	IPSEC	N/A	9991234567	Tunnel	N/A	0	0	
	Duration: 0 hrs 00 mins 02 secs									
2001/01/19 10:45:24		kparadis	IPSEC-HTTPS	N/A	9991234567	Tunnel	N/A	0	0	
2001/01/19 12:05:58	2001/01/19 12:06:31	kparadis	IPSEC-HTTPS	N/A	9991234567	Tunnel	N/A	0	0	
	Duration: 0 hrs 00 mins 33 secs									
2001/01/19 12:10:16	2001/01/19 12:10:40	kparadis	IPSEC-HTTPS	N/A	9991234567	Tunnel	N/A	0	0	
	Duration: 0 hrs 00 mins 24 secs									
2001/01/19 12:17:04	2001/01/19 12:17:10	kparadis	IPSEC	N/A	9991234567	Tunnel	N/A	0	0	
	Duration: 0 hrs 00 mins 06 secs									
2001/01/19 12:18:30	2001/01/19 12:20:55	kparadis	IPSEC	N/A	9991234567	Tunnel	N/A	0	0	

Figure 97 Client Session Details Report

Accounting Report

This report lists all tunnel sessions that occurred during the selected period, sorted by user name. In addition to a wide range of tunnel performance statistics for each session, this report indicates the virtual subnet IP address allocated to the remote client, the duration of each session, and the reason the session ended. Possible reasons the session ended include:

- ❐ *User Request*: the Aurorean user pressed Disconnect to disconnect the tunnel; this is the most common reason for a session to end.
- ❐ *Lost Service*: the tunnel was disconnected unexpectedly, such as when the Aurorean PC reboots without warning or when the dial-up connection between Aurorean and the ISP POP ends abruptly.
- ❐ *User Error*: the Aurorean Network Gateway and Aurorean Client were unable to successfully negotiate a tunnel connection.

In addition to the data described below, throughput, login and session totals are reported for each client as well as the reason for why the session ended. This report also offers a drill-down view in a subsequent display. Table 17 lists the column headings and values that appear in an Accounting Report.

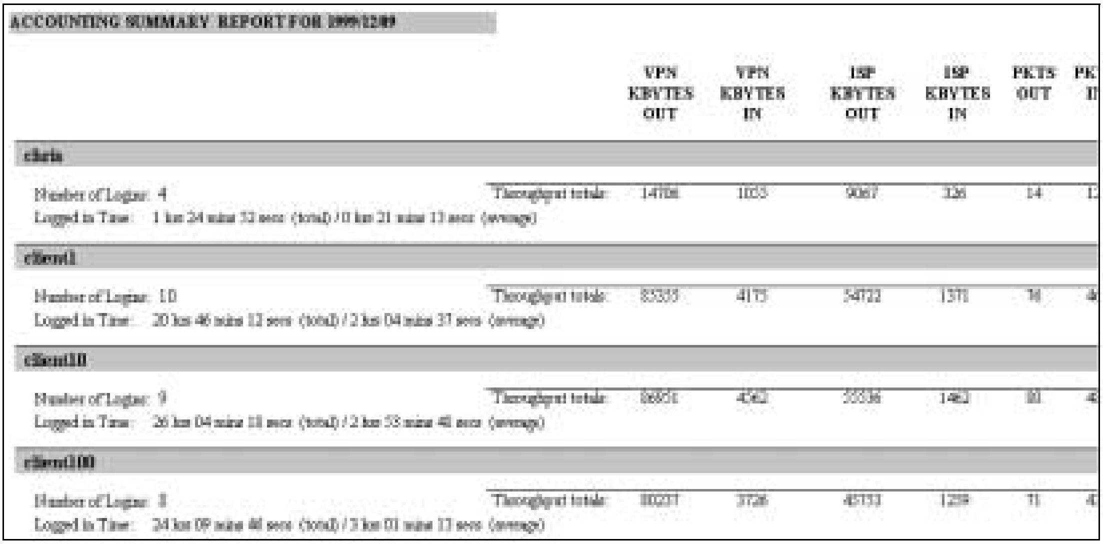
Table 17 Accounting Report Values

Heading	Explanation
TIME IN	Time the tunnel session started (according to the ANG's clock) in the format: *Year*/*Month*/*Day Time* where *Time* is shown in military time.
TIME OUT	Time the tunnel session ended (according to the ANG's clock) in the format: *Year*/*Month*/*Day Time* where *Time* is shown in military time.
PROTOCOL	Tunnel protocol negotiated for the session (IPSec or PPTP).
VIRTUAL IP ADDRESS	IP address allocated from a virtual subnet to the remote client during the session.
PHYSICAL IP ADDRESS	IP address of the Ethernet port on the ANG that accepted the tunnel session (typically the External port).

Table 17 Accounting Report Values

Heading	Explanation
VPN KBYTES OUT	Total bytes of data sent end-to-end over the tunnel from the corporate network to the Aurorean user during the session.
VPN KBYTES IN	Total bytes of data sent end-to-end over the tunnel from the Aurorean user to the corporate network during the session.
ISP KBYTES OUT	Total bytes of data sent from the ISP POP to the Aurorean user during the session.
ISP KBYTES IN	Total bytes of data sent from the Aurorean user to the ISP POP during the session.
PKTS OUT	Total number of packets transmitted over all tunnels from the ANG. Packets are shown in terms of total counts and packets per second throughput.
PKTS IN	Total number of packets received over all tunnels by the ANG Packets are shown in terms of total counts and packets per second throughput.
PKTS RETRNS	Total number of packets retransmitted because they were received out of order.
DUP PKTS	Total number of packets received which were duplicates of previously received packets.
LOST PKTS	Number of packets dropped during the session due to flow control or checksum errors.
User # of logins	Number of logins by the specified user
Total time	Total interval of time the specified user was logged in
Average login time	Average session time of specified user

Figure 98 displays a typical Accounting Summary Report.

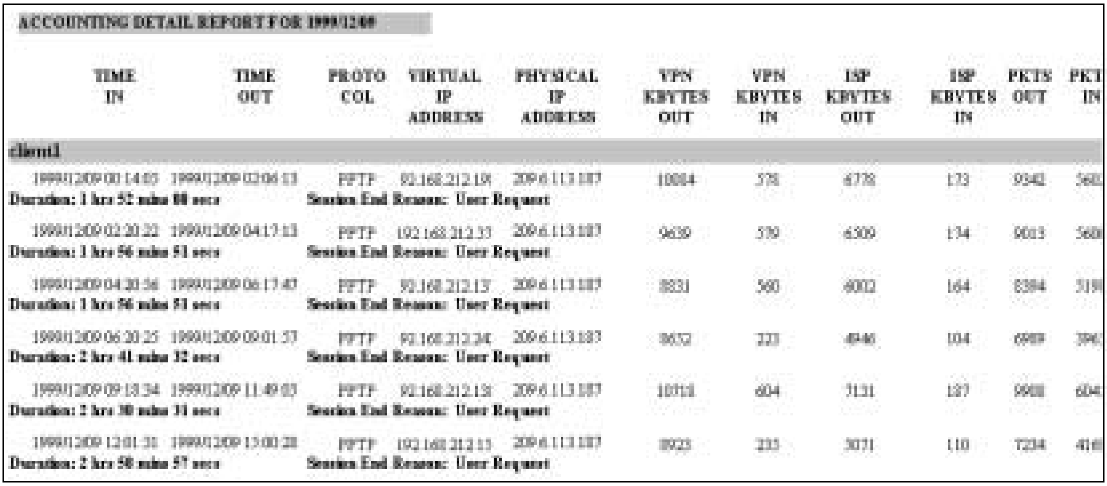


ACCOUNTING SUMMARY REPORT FOR 1999/12/09

		VPN KBYTES OUT	VPN KBYTES IN	ISP KBYTES OUT	ISP KBYTES IN	PKTS OUT	PK I
chris							
Number of Logins: 4 Logged in Time: 1 hrs 24 mins 53 secs (total) / 0 hrs 21 mins 13 secs (average)	Throughput totals:	14706	1053	9067	326	14	1
client1							
Number of Logins: 10 Logged in Time: 20 hrs 46 mins 12 secs (total) / 2 hrs 04 mins 37 secs (average)	Throughput totals:	83535	4175	54722	1371	76	4
client10							
Number of Logins: 9 Logged in Time: 26 hrs 04 mins 18 secs (total) / 2 hrs 53 mins 48 secs (average)	Throughput totals:	86851	4562	55336	1462	81	4
client100							
Number of Logins: 8 Logged in Time: 24 hrs 09 mins 48 secs (total) / 3 hrs 01 mins 13 secs (average)	Throughput totals:	80237	3726	45753	1259	71	4

Figure 98 Accounting Summary Report

Double-clicking on the client1 user name line above with the magnifier icon produces a drill-down Accounting Detail Report similar to Figure 99 below.



ACCOUNTING DETAIL REPORT FOR 1999/12/09

TIME IN	TIME OUT	PROTO COL	VIRTUAL IP ADDRESS	PHYSICAL IP ADDRESS	VPN KBYTES OUT	VPN KBYTES IN	ISP KBYTES OUT	ISP KBYTES IN	PKTS OUT	PKT IN
client1										
1999/12/09 00:14:05	1999/12/09 02:06:13	PPTP	92.168.212.19	209.6.113.187	10084	578	6778	173	9542	560
Duration: 1 hrs 52 mins 08 secs		**Session End Reason: User Request**								
1999/12/09 02:20:22	1999/12/09 04:17:13	PPTP	192.168.212.33	209.6.113.187	9639	579	6309	134	9013	560
Duration: 1 hrs 56 mins 51 secs		**Session End Reason: User Request**								
1999/12/09 04:20:56	1999/12/09 06:17:47	PPTP	92.168.212.13	209.6.113.187	8831	560	6002	164	8394	519
Duration: 1 hrs 56 mins 51 secs		**Session End Reason: User Request**								
1999/12/09 06:20:25	1999/12/09 09:01:57	PPTP	92.168.212.24	209.6.113.183	8652	223	4946	104	6989	396
Duration: 2 hrs 41 mins 32 secs		**Session End Reason: User Request**								
1999/12/09 09:13:34	1999/12/09 11:49:03	PPTP	92.168.212.18	209.6.113.187	10718	604	7131	137	9908	604
Duration: 2 hrs 36 mins 31 secs		**Session End Reason: User Request**								
1999/12/09 12:01:31	1999/12/09 15:00:28	PPTP	192.168.212.15	209.6.113.187	8923	233	3071	110	7234	416
Duration: 2 hrs 58 mins 57 secs		**Session End Reason: User Request**								

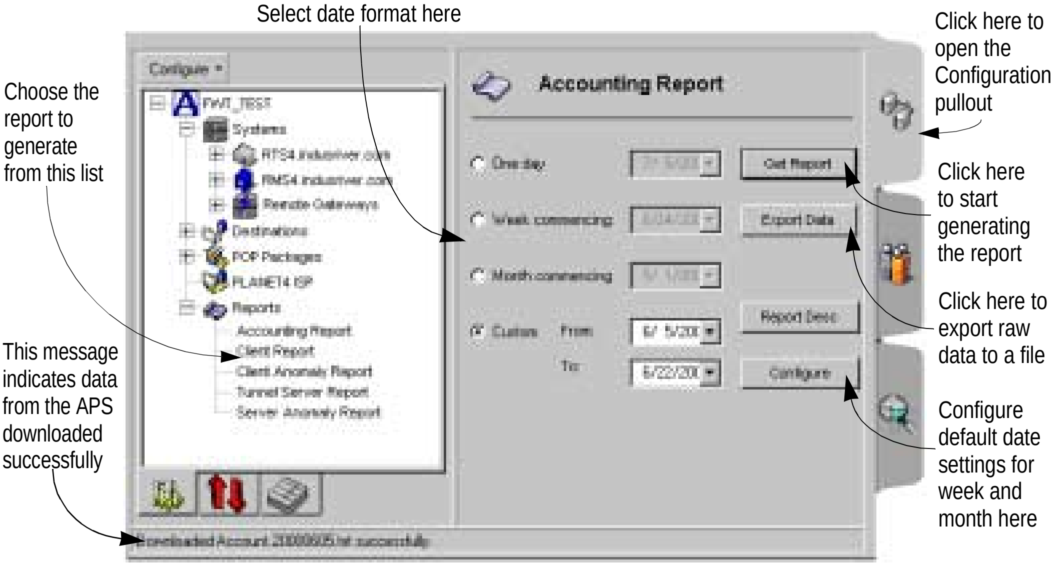
Figure 99 “Drill-down” Accounting Detail Report

Downloading, Viewing and Exporting Reports

To download and view, print or export a report, perform the following steps:

1. Open the Configuration pullout.
2. Expand the list under Reports by clicking the + symbol.
3. Choose the type of report you want to download and view.

   Figure 100 shows the Accounting Report display. For a detailed description of any selected report type, click Report Description.



Downloaded Account 20000605.txt successfully

Select date format here

Choose the report to generate from this list

This message indicates data from the APS downloaded successfully

Click here to open the Configuration pullout

Click here to start generating the report

Click here to export raw data to a file

Configure default date settings for week and month here

Figure 100 Accounting Report Display

4. Choose from daily, weekly, monthly or custom options.

   By default, the previous day constitutes the One day period and Sunday marks the beginning of the week. Also, weeks and months commence on the first *full* week or month. If you want to choose an irregular period, click Custom. Also, you may set your own default periods by clicking Configure and selecting a date from the pop-up window.

NOTE

Because source data appearing in each daily report is not collected by the APS until the end of the day, you cannot generate a report for the current day.

5 Do one of the following:

- Click Get Report to start generating the report. RiverMaster sends the report request to the APS which FTPs the file to the RiverMaster computer. To vary the width of the report, select a value in the percentage field. After the report appears, you can double-click the magnifier icon on a user's name to focus on user-specific data.
- Click Export Data if you want to simply export the data in flat ASCII text without viewing the report. A Save As window appears prompting you to select the directory to store this file.

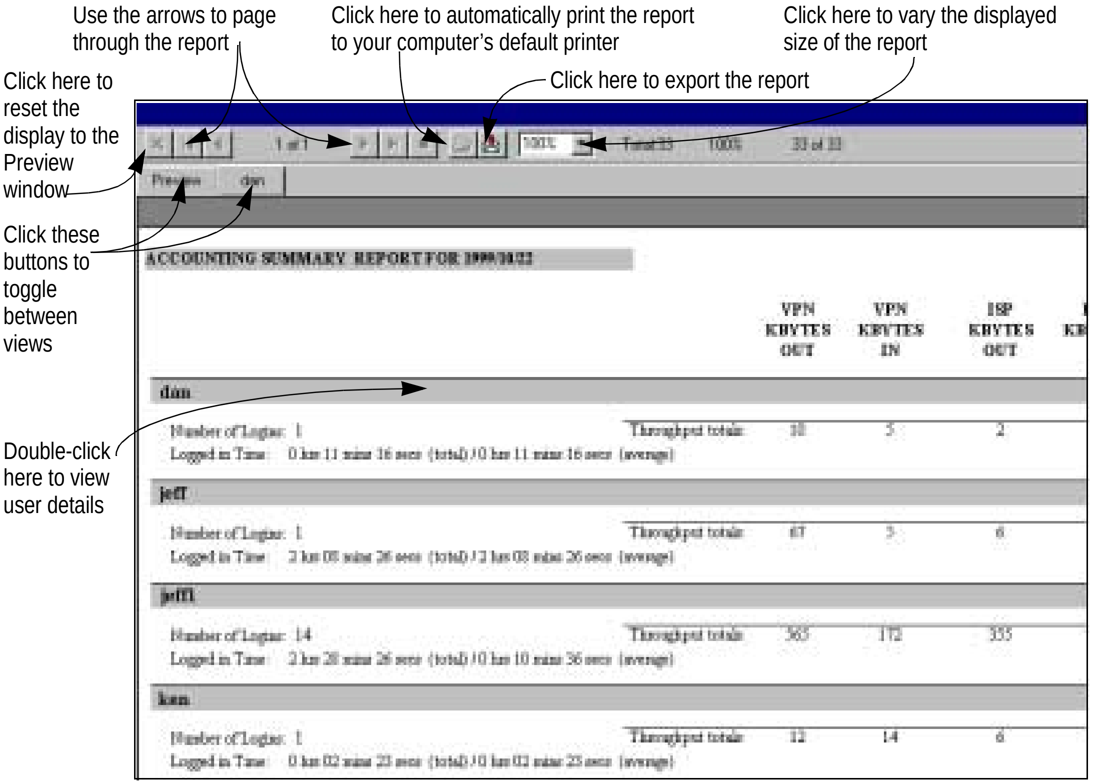
NOTE

Depending upon the level of activity and interval queried, you may need to wait a while for a report viewing window to appear as shown in Figure 101. For example, an Accounting Report for 1000 sessions may take 10 minutes or more to download. For reports which cover hundreds of logins or many weeks of heavy activity, the report viewing window appears blank and the hourglass which usually indicates activity also disappears while data is being compiled.

CAUTION

If you run two sessions of RiverMaster, do not generate the same type of report on both sessions at the same time. If you require the same report from both RiverMasters, wait until one report is finished compiling before starting the second report.

6 If you chose Export Data, you may keep the default file name or type a new name, select the directory and click Save. Optionally, you can select another file type by clicking the Save as type down arrow.



Use the arrows to page through the report

Click here to automatically print the report to your computer's default printer

Click here to vary the displayed size of the report

Click here to export the report

Click here to reset the display to the Preview window

Click these buttons to toggle between views

Double-click here to view user details

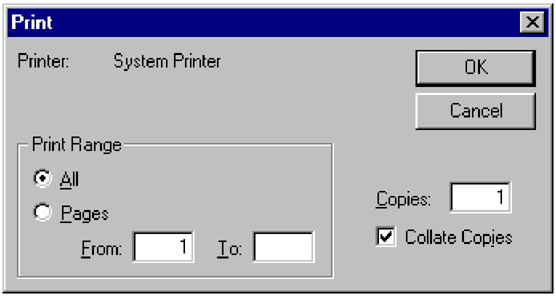
ACCOUNTING SUMMARY REPORT FOR 1998/10/22

		VPN KBYTES OUT	VPN KBYTES IN	ISP KBYTES OUT	KB
dan					
Number of Logins: 1	Throughput totals:	10	5	2	
Logged in Time: 0 hrs 11 mins 16 secs (total) / 0 hrs 11 mins 16 secs (average)					
jeff					
Number of Logins: 1	Throughput totals:	67	3	6	
Logged in Time: 2 hrs 08 mins 26 secs (total) / 2 hrs 08 mins 26 secs (average)					
jeff1					
Number of Logins: 14	Throughput totals:	365	172	335	
Logged in Time: 2 hrs 28 mins 26 secs (total) / 0 hrs 10 mins 36 secs (average)					
ken					
Number of Logins: 1	Throughput totals:	12	14	6	
Logged in Time: 0 hrs 02 mins 23 secs (total) / 0 hrs 02 mins 23 secs (average)					

Figure 101 Report Viewing Window

Printing Reports

To print reports, you must have a default printer defined for your computer. Click the printer button along the top edge of the report display. A Print window appears as shown in Figure 102; set the printing options and click OK.



Printer: System Printer

Print Range
● All
○ Pages
From: 1 To:

Copies: 1
☑ Collate Copies

Figure 102 Report Print Window

NOTE

If you do not have at least one printer driver installed on your computer, the printer button is disabled. To install a printer, follow the instructions provided in Windows on-line Help.

Exporting Reports

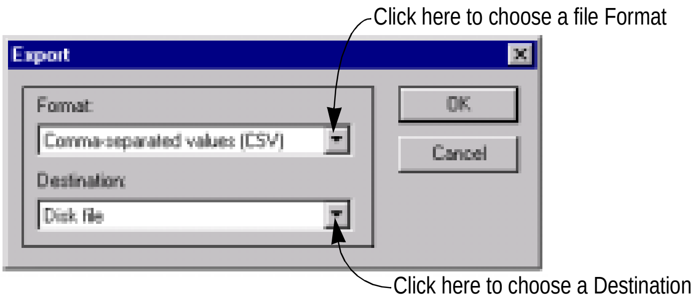
Aurorean Virtual Network supports the exporting of reports in more than a dozen formats to either a file on disk, a Microsoft Exchange folder, or your mail server via the Microsoft Application Programming Interface (MAPI) program. This feature differs from the export option offered in the report display windows which dumps raw data into a file in ASCII format.

Exporting Reports to a Disk File

To export reports to a disk file, perform the following steps:

1 Click the Export button along the top edge of the report display.

The Export window appears as shown in Figure 103.



Format: Comma-separated values (CSV)

Destination: Disk file

Click here to choose a file Format

Click here to choose a Destination

Figure 103 Export Window

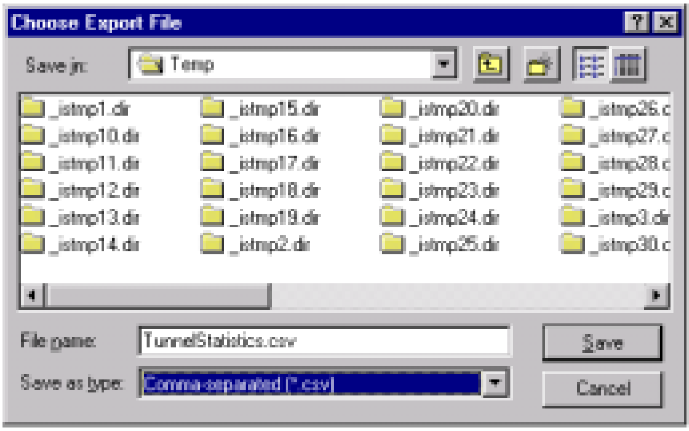
2 Select Disk file in the Destination field.

You may also export the report to a file in a Microsoft Exchange folder, or to your mail server using MAPI. Refer to “Exporting Reports to a Microsoft Exchange Folder” on page 203 or “Exporting Reports Using MAPI” on page 207 for more information.

3 Select a program file Format to export the report in and click OK. Refer to the table below to begin.

If you want this export format ...	Go to ...
Crystal Reports Excel versions 2.1, 3.0, 4.0, or 5.0 Lotus 1-2-3 (all versions) Rich Text Format Tab-separated text Text Word for Windows	Step 4
All HTML versions	Step 6
Character-separated values	Step 8
Data Exchange Format Tab-separated values Record Style Comma-separated values	Step 9
ODBC versions: Account.txt ClAnom.txt Client.txt DBASE Files Fox Pro Files PHD_Files_32 bit SvrAnom.txt Text Files TnlServr.txt.	Step 11
ODBC versions: Excel Files MS Access 97 Database	Step 13
Paginated Text	Step 15
Excel 5.0 Tabular	Step 16

4 If you selected one of the following formats: Crystal Reports, Excel versions 2.1, 3.0, 4.0, or 5.0, Lotus 1-2-3, Rich Text Format, Tab-separated text, Text, or Word for Windows, the Choose Export File appears immediately as shown in Figure 104. Choosing other formats may bring up this window after performing the initial step.



Save in: Temp

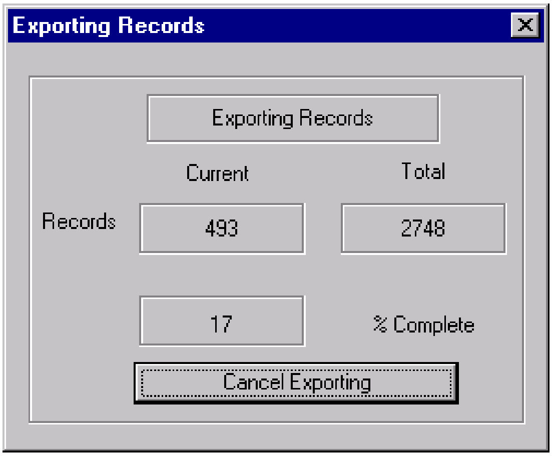
File name: TunnelStatistics.csv

Save as type: Comma-separated (*.csv)

Figure 104 Choose Export File Window

5 Select the directory to store the report and click Save. Optionally, you may also rename the file or save it in a different format.

The Exporting Records window appears as shown in Figure 105. This window is a running tally of the number of records exported and percentage of the job completed. Optionally, you may click Cancel Exporting if necessary. When the % Complete percentage reaches 100, the export is completed. Optionally, you can click Cancel Exporting.



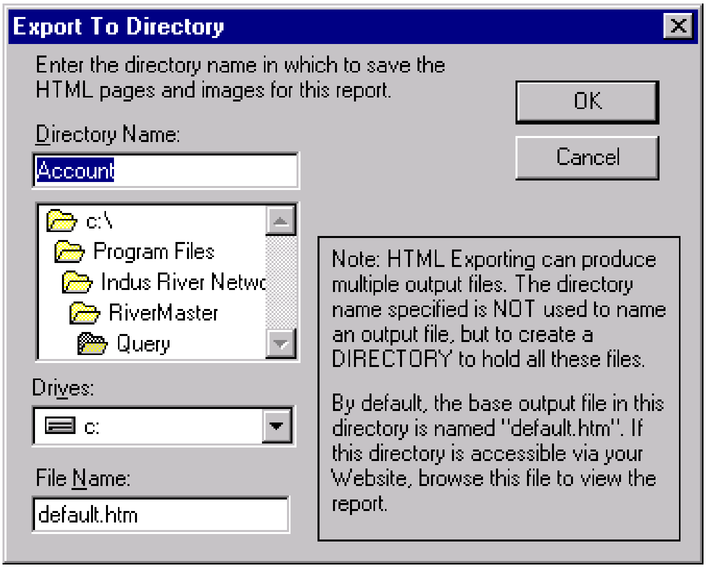
	Current	Total
Records	493	2748

17 % Complete

Figure 105 Exporting Records Window

6 If you selected HTML versions 3.0, 3.2 Extended or 3.2 Standard, you are prompted to specify the name of a directory where the report - titled `default.htm` - will be written.

The Export To Directory window appears as shown in Figure 106.



Export To Directory

Enter the directory name in which to save the HTML pages and images for this report.

Directory Name: Account

Drives: c:

File Name: default.htm

Note: HTML Exporting can produce multiple output files. The directory name specified is NOT used to name an output file, but to create a DIRECTORY to hold all these files.

By default, the base output file in this directory is named "default.htm". If this directory is accessible via your Website, browse this file to view the report.

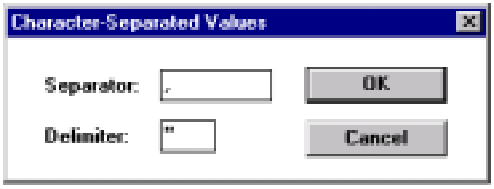
Figure 106 Export To Directory Window

7 Enter a Directory Name and click OK to export the file to the default directory shown or search the directory and Drives fields for the desired destination and click OK.

The Exporting Records window appears as shown in Figure 105. Return to Step 4 to continue.

8 If you chose Character-separated values, you are prompted to enter characters to separate and delimit the output text. Accept the defaults or set new values and click OK.

The Character-Separated Values dialog box appears as shown in Figure 107. The delimiter sets the start or end of a portion of text while the separator visually breaks those portions. When finished, continue with Step 9.

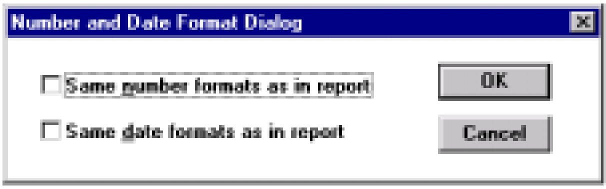


Separator: ,
Delimiter: "

Figure 107 Character-Separated Values Dialog Box

9 If you selected Character-, Tab- or Comma-separated values, Data Exchange Format, or Record Style, you are prompted to retain the number and date formats presently in the report.

The Number and Date Format Dialog box appears as shown in Figure 108.



☐ Same number formats as in report
☐ Same date formats as in report

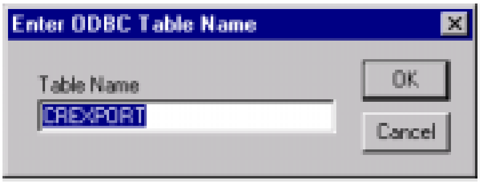
Figure 108 Number and Date Format Dialog Box

10 Checkmark the applicable boxes if you want to keep either of these formats or leave them blank and click OK.

The Choose Export File window appears as shown in Figure 104. Return to Step 4 to continue.

11 If you selected the following versions of ODBC: Account.txt. ClAnom.txt, Client.txt, DBASE Files, Fox Pro Files, PHD_Files_32 bit, SvrAnom.txt, Text Files, or TnlServr.txt., you are prompted to enter a name for the ODBC table.

The Enter ODBC Table Name dialog box appears as shown in Figure 109.



CREXPORT

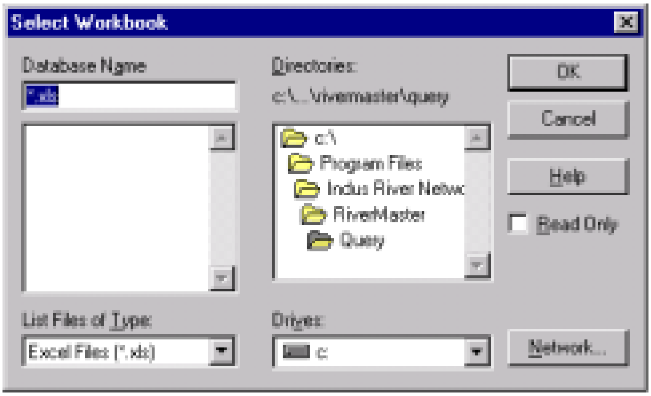
Figure 109 Enter ODBC Table Name Dialog Box

12 Type a name for the ODBC table in the field provided and click OK.

The Exporting Records window appears as shown in Figure 105. Return to Step 4 to continue.

13 If you selected the Excel Files or MS Access 97 Database versions of ODBC, you are prompted to select a database name and location for the .XLS file (Excel) or .MDB file MS Access.

The Select Workbook Window (Excel) appears as shown in Figure 110. The Select Database window (MS Access 97) appears substantially the same.



Select Workbook

Database Name: *.xls

Directories: c:\...\rivermaster\query

List Files of Type: Excel Files (*.xls)

Drives: c:

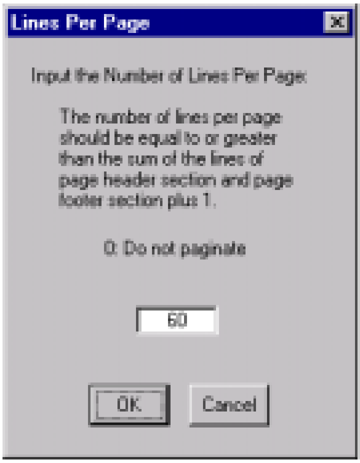
Figure 110 Select Workbook Window

14 Type an ODBC database name in the field provided and click OK.

The Exporting Records window appears as shown in Figure 105. Return to Step 4 to continue.

15 If you chose the Paginated Text format, you are prompted to set the number of lines per page or keep the default of 60 lines and click OK.

The Lines Per Page dialog box appears as shown in Figure 111. The Choose Export File window follows as shown in Figure 104. Return to Step 4 to continue.



Input the Number of Lines Per Page:

The number of lines per page should be equal to or greater than the sum of the lines of page header section and page footer section plus 1.

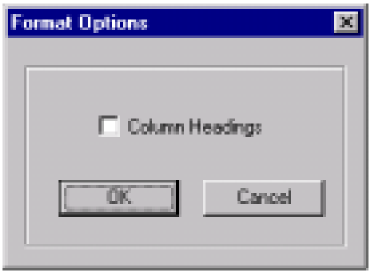
0: Do not paginate

60

Figure 111 Lines Per Page Dialog Box

16 If you chose the Excel 5.0 Tabular format, you are prompted to set column headings. Check the box or leave it blank and click OK.

The Format Options dialog box appears as shown in Figure 112. The Choose Export File window follows as shown in Figure 104. Return to Step 4 to continue.



□ Column Headings

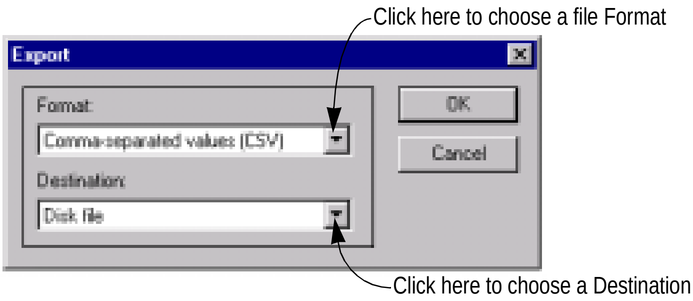
Figure 112 Format Options Dialog Box

Exporting Reports to a Microsoft Exchange Folder

To export reports to a Microsoft Exchange folder, perform the following steps:

1 Click the Export button along the top edge of the report display.

The Export window appears as shown in Figure 103.



Format: Comma-separated values (CSV)

Destination: Disk file

Click here to choose a file Format

Click here to choose a Destination

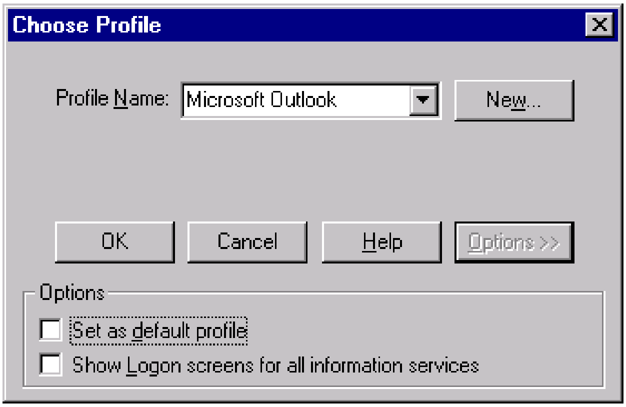
Figure 113 Export Window

2 Select a program file Format that the report will be exported in by clicking the arrow under the Format field.

You may convert the report to a file in one of the following formats: Comma-separated values (CSV), Character-separated values, Crystal Reports (RPT), Data Exchange Format (DIF), Microsoft Excel (XLS), Hyper Text Markup Language (HTML), Lotus 1-2-3 (WK1, WK3, WKS), Open Database Connectivity (ODBC), Paginated Text (TXT), Record Style (REC), Rich Text Format (RTF), Tab-separated text (TTX), Tab-separated values (TSV), Text (TXT), and Word for Windows (DOC).

3 Select Exchange Folder in the Destination field and click OK.

The window that appears will depend on your selected format. Go to the “Exporting Reports to a Disk File” section and find the starting step for the format you selected. When you complete the next step or two, the Choose Profile window appears as shown in Figure 114. If you have not created a user profile, use the Profile Wizard to do so. Optionally, you may export the report to your mail server using MAPI. Refer to “Exporting Reports Using MAPI” on page 207.



Profile Name: Microsoft Outlook

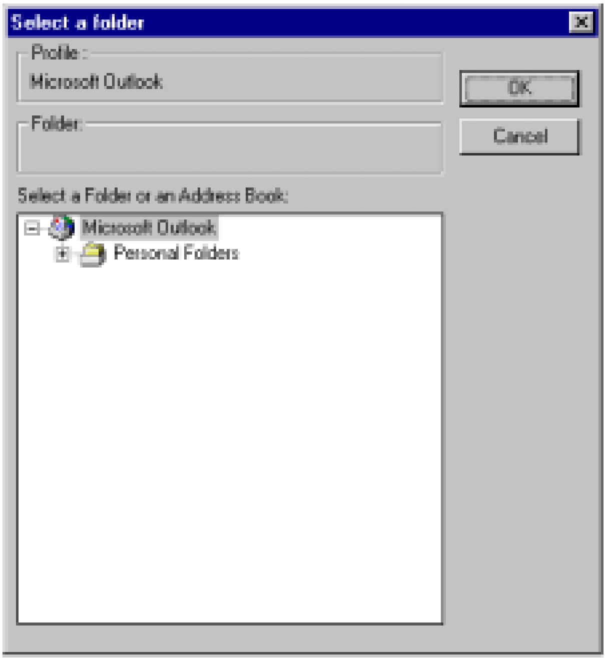
□ Set as default profile

□ Show Logon screens for all information services

Figure 114 Choose Profile Window

4 Select a Profile Name by clicking the arrow next to the field and click OK. You can also create a new profile or configure two options.

The Select a folder window appears as shown in Figure 115.



Profile : Microsoft Outlook

Folder:

Select a Folder or an Address Book:

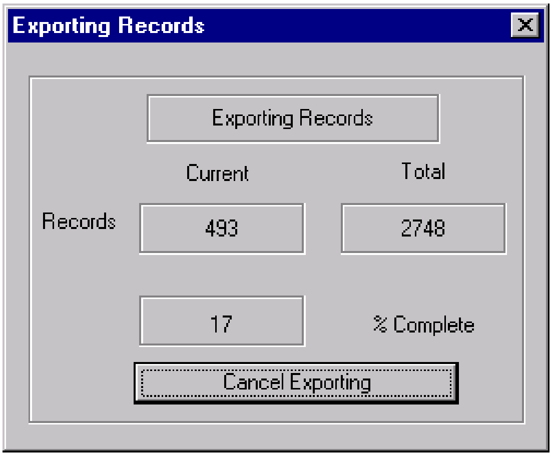
- Microsoft Outlook
  - Personal Folders

Figure 115 Select a Folder Window

5 Click on a folder to store the report and click OK.

The Exporting Records window appears as shown in Figure 116. This window is a running tally of the number of records exported and percentage of the job completed. Optionally, you may click Cancel Exporting if necessary.

When the % Complete percentage reaches 100, the export is completed. Optionally, you can click Cancel Exporting.



	Current	Total
Records	493	2748
	17	% Complete

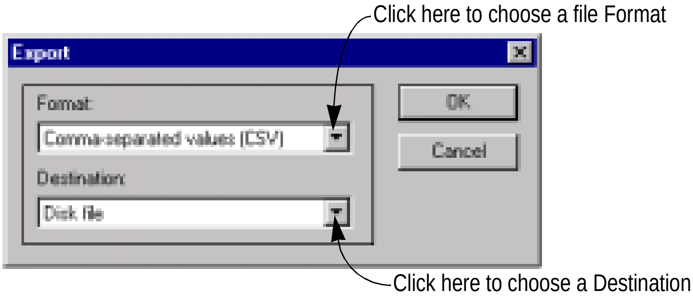
Figure 116 Exporting Records Window

Exporting Reports Using MAPI

To export reports to your mail server using MAPI, perform the following steps:

1. Click the Export button along the top edge of the report display.

   The Export window appears as shown in Figure 117.



Export

Format:

Comma-separated values (CSV)

Destination:

Disk file

OK
Cancel
Click here to choose a file Format
Click here to choose a Destination

Figure 117 Export Window

2. Select a program file Format to export the report in by clicking the arrow under the Format field.

   You may convert the report to a file in one of the following formats: Comma-separated values (CSV), Character-separated values, Crystal Reports (RPT), Data Exchange Format (DIF), Microsoft Excel (XLS), Hyper Text Markup Language (HTML), Lotus 1-2-3 (WK1, WK2, WKS), Open Database Connectivity (ODBC), Paginated Text (TXT), Record Style (REC), Rich Text Format (RTF), Tab-separated text (TTX), Tab-separated values (TSV), Text (TXT), and Word for Windows (DOC).

3. Select Microsoft Mail (MAPI) in the Destination field and click OK.

   The window that appears will depend on your selected format. Go to the "Exporting Reports to a Disk File" section and find the starting step for the format you selected. When you complete the next step or two, the Choose Profile window will appear for all formats selected as shown in Figure 118.

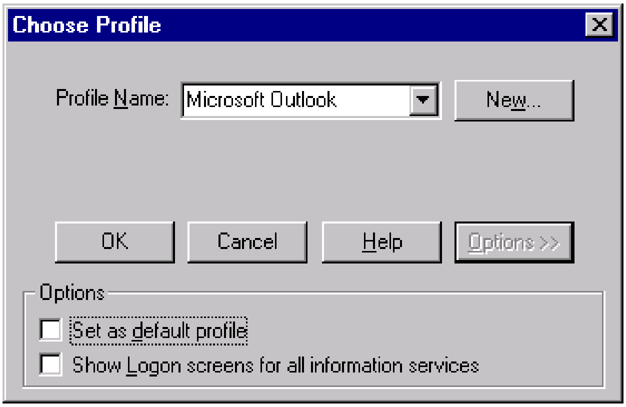


Figure 118 Choose Profile Window

4 Select a Profile Name by clicking the arrow next to the field and click OK. You can also create a new profile or configure two options.

The Send Mail window appears as shown in Figure 119.

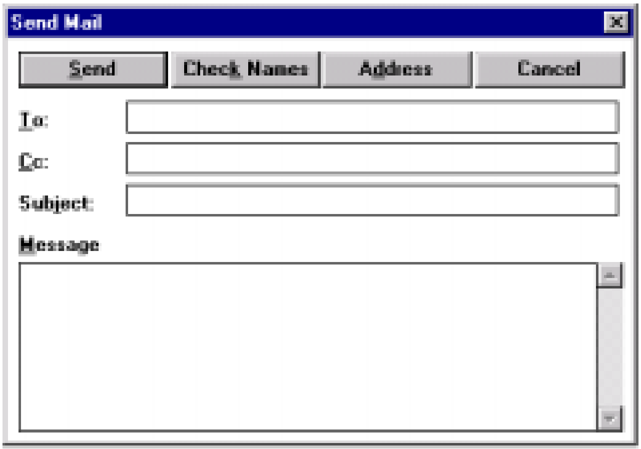


Figure 119 Send Mail Window

5 Fill in the open fields as you would any mail message and click Send.

The export is now complete.

A

Glossary

Aurorean Client Software

Enterasys Networks client software that runs on a Windows 95/98/NT computer that allows a remote user to create a secure tunneling connection to a corporate network. This application features the TollSaver database that automatically presents a list of ISP POP's to allow the user to select the lowest-cost connection, and the Prescriptive Diagnostics Engine that automatically diagnoses connection problems and either corrects the problem itself or directs the remote user on how to solve the problem.

Aurorean Network Gateway

An Enterasys Networks device that creates a secure virtual private circuit over the Internet between itself and a remote user's computer. The Aurorean Network Gateway encapsulates data packets using PPTP and encrypts data to prevent third-parties from intercepting and examining it. A Aurorean Network Gateway receive its configuration settings from a Aurorean Policy Server and passes login information to the Aurorean Policy Server when a remote user attempts to authenticate a tunnel connection.

Aurorean Policy Server

An Enterasys Networks device that manages Aurorean Network Gateways. Network administrators configure Aurorean Policy Servers from a RiverMaster computer. The network administrator can create a remote user database on the Aurorean Policy Server or instruct the Aurorean Policy Server to authenticate remote users against an external authentication server (such as a RADIUS or SecurID server). When the network administrator changes tunnel connection parameters, the Aurorean Policy Server provide updated configuration files to Aurorean Network Gateways on request.

AutoLink Recovery

An extension of the fault recovery capabilities of the Aurorean Client which includes automatic fail-over to a backup Aurorean Client system in the event of a service outage or VPN hardware failure. AutoLink Recovery (ALR) is implemented with the installation of a second Aurorean Client system consisting of a pair of Aurorean Policy Servers and Aurorean Network Gateways. The secondary Aurorean Client system operates in parallel with but independently of the primary Aurorean Client system. Each system must be located on the same corporate network, but can be physically situated at different sites for disaster recovery. For more information about ALR, refer to the ALR *Application Note*.

Client Synchronization

A two-part process which automatically upgrades Aurorean Client firmware and settings by downloading updated files from the Aurorean Policy Server. During client synchronization, a portion of the tunnel is utilized as a management channel between the Aurorean Client computer and the Aurorean Policy Server, operating in the “background” of the client connection without any visible effect on performance. *Data Synchronization* acquires revised POP, ISP, policy and other configuration data while *Software Synchronization* acquires new Prescriber remedies and updated Aurorean Client program files.

Firewall

A combination of hardware and software which limits the exposure of a corporate network to outside attack by enforcing a boundary between the network and the Internet. Firewalls normally fall into one of two categories: application-level or network-level (often referred to as a packet filter). An application-level firewall examines traffic at the application level, and only passes packets that are sent by approved applications (such as FTP, E-mail, or Telnet). This type of firewall often readdresses outgoing traffic so that it appears to have originated at the firewall rather than an internal host, thereby concealing the address of the internal host. A network-level firewall examines traffic at the network packet level, and filters packets based on the destination and / or source address. The Aurorean Network Gateway offers Firewall/NAT Traversal as a policy option to Aurorean Client users such as contractors, visitors and others, who are connected temporarily on internal networks, permitting them to dial out of the network across the firewall to their own corporate network and returning to their computer. Aurorean Client uses this feature in conjunction with the HyperText Transfer Protocol Secure (HTTP-S) to successfully traverse the firewall without causing harm to the native network.

Generic Routing Encapsulation (GRE)

Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link over the Internet. For PPTP, GRE is used to encapsulate PPP data packets within an IP packet (IP packet headers contain address information necessary for routing, while PPP packets do not).

Internet Service Provider (ISP)

A vendor who provides direct access to the Internet. ISPs bill users for the amount of time they are connected, and may also offer additional services such as Web site hosting, E-mail, or news group readers. Remote users reach the ISP by dialing into an ISP POP with a computer, modem, and phone line, or over a dedicated circuit (such as a cable modem connection).

Management Channel

A portion of the tunnel connection that is used to download an updated TollSaver database from the Aurorean Policy Server to the Aurorean Client computer. When a remote user establishes a tunnel connection to the corporate network, Aurorean Client sends a message to the Aurorean Policy Server asking if the TollSaver database has changed. If the Aurorean Client's database is out-of-date, the Aurorean Policy Server downloads a new database during low-traffic periods, so that the download does not interfere with regular traffic between the remote user and the network.

Network Address Translation (NAT)

Described by Whatis.com as the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This provides security since each outgoing or incoming request must undergo a translation process that also offers the chance to qualify or authenticate the request or match it with a previous request. NAT also conserves the number of global IP addresses that a company uses and permits the use of a single IP address to interface with the world. RiverMaster permits the Aurorean Network Gateway to be configured as a NAT server. The ANG also offers Firewall/NAT Traversal as a policy option to Aurorean Client users such as contractors, visitors and others, who are connected temporarily on internal networks, permitting them to dial out of the network across the firewall to their own network and return to their computer. Aurorean Client uses this feature in conjunction with the HyperText Transfer Protocol Secure (HTTP-S) to successfully traverse the NAT server without causing harm to the native network.

Network Administrator

The person responsible for installing and maintaining a company’s network equipment, and also insuring that network resources (such as servers and the applications running on them) are consistently available and performing well. In terms of Enterasys Networks products, this person physically installs Aurorean Policy Servers and Aurorean Network Gateways, distributes Aurorean Client to remote users, and runs RiverMaster software on his/her computer to manage the entire VPN.

Point of Presence (POP)

In Internet terms, the physical site that contains an ISP’s network equipment. Remote users dial into the POP, authenticate against the ISP’s customer database, and then gain access to the Internet. ISPs typically have POPs scattered throughout their service area, so that can customers can dial a local phone call and avoid paying long-distance charges when accessing the Internet.

Point-to-Point Protocol (PPP)

The Internet standard for sending network traffic over serial lines, such as dial-up phone lines. Unlike its predecessor SLIP (Serial Line Internet Protocol), PPP provides error detection and compression capabilities.

Point-to-Point Tunneling Protocol (PPTP)

A network protocol for linking remote locations over the Internet rather than over costly long-distance or leased lines. To accomplish this, PPTP encapsulates other network protocols (such as TCP/IP, IPX, and NetBEUI) and uses encryption to secure the data sent over the Internet. PPTP was developed jointly by Microsoft and U.S. Robotics (3Com).

Policy

A set of rules that governs how remote users log onto the corporate network. Corporate policies are defined by the network administrator and maintained on the Aurorean Policy Server. Policies fall into two general categories: Internet access and user/group administration. For Internet access, the network administrator determines which ISPs and telephone carriers the remote user can select, what rates are acceptable for phone calls and Internet connection periods, and which regions of the country the remote user may connect from. These policies are reflected in the customized TollSaver database that is distributed as part of the Aurorean Client. For user/group administration, the network administrator establishes the log in methods for both ISP access and corporate network access; specifies the use of protocols, encryption, and compression; and determines the user's right to change his or her username or password.

POP Package

A set of ISPs that can be assigned to one or more client groups. RiverMaster creates a POP package as the first, most time-consuming step of the Aurorean Client Installation Kit build when the TollSaver database is generated. The second step of the kit build incorporates configuration values for the system with the POP package and its associated ISPs.

Prescriber

A feature of Enterasys Networks products that diagnoses why a tunnel connection failed and attempts to correct the problem, either on its own or with user assistance. On Enterasys Networks Aurorean Client, the Prescriptive Diagnostics Engine performs a step-by-step check of each tunnel connection element, including the COM port or serial driver used, modem or terminal adapter, line to a PBX or the telephone network, local or long distance phone service, connection to the ISP POP, ISP authentication settings, and so forth. On the Enterasys Networks Aurorean Policy Server, the Prescriptive Diagnostics Engine uses the call home feature to provide an alternate route that tests end-to-end operation and isolates tunnel problems, and also allows the remote user to download missing or updated files.

Remote Client/User

A computer user who wants to access data on a corporate network from a remote location, such as a field office, home office, or temporary lodging. Remote users working from a fixed location are often referred to as telecommuters or day-extenders (if they access the network after regular work hours). Remote users who travel frequently and attempt to access the network from different locations are often called mobile users.

RiverMaster

A management application running on a Windows NT 4.0 Workstation / 2000 Professional computer which communicates with Aurorean Policy Servers and Aurorean Network Gateways. Using RiverMaster, a network administrator creates user databases, sets policies for user groups, views activity logs, and generates usage reports.

Routers

Devices which direct network traffic among LANs or WANs until the data reaches its destination. To do this, routers communicate with one another using dedicated protocols such as IGRP (Interior Gateway Routing Protocol) and BGP (Border Gateway Protocol) to transfer information on network addressing, status, and configuration.

Thread

Described by Microsoft as an executable entity that belongs to a single process, a thread in Aurorean Client is a login process. In RiverMaster, you can increase the number of threads to permit more authentications by users attempting to connect simultaneously. The IR Authentication service is the only multi-threaded process that can be configured as such in Aurorean Client.

TollSaver Database

A feature of Enterasys Networks products that provides remote users with a list of ISPs, phone numbers of available POPs, and connection rates. The master TollSaver database is maintained on the Aurorean Policy Server and downloaded to the Aurorean Client over the management channel portion of the tunnel connection.

Tunneling

Technology that lets a network transport protocol carry information for other protocols within its own packets. For example, by encapsulating NetBEUI packets, IP can route them across the Internet, which is not normally possible.

Virtual Private Network (VPN)

An extension of a company’s private network that uses the resources of the public Internet. While most private networks use dedicated lines and equipment that are company property, a virtual private network “borrows” resources from the Internet on an as-needed basis.

B

ANG-3000/7000 Preconfiguration Stored on a Floppy Disk

This appendix describes how to preconfigure the Aurorean Network Gateway (ANG-3000 / 7000) using a floppy disk to store the configuration. This procedure is similar to configuring the ANG using the RiverMaster application. But this method allows an administrator to centrally configure one or more gateways and conveniently distribute that configuration data on floppy disks to remote sites.

When the floppy disk is inserted in the Remote ANG and the ANG rebooted, configuration information stored in the `config.irx` file is copied and the ANG is ready to initiate tunnels. To enable the ANG to terminate tunnels. please use the Aurorean Policy Manager as described in Chapter 3 of the *Aurorean Installation & Service Guide.*

Also, any initiating ANG User configured here must later be added to the User and Group database of the Local ANG. Refer to Chapter 6, “Managing Users and Groups,” of this manual for instructions. ANG configuration with a floppy disk is organized sequentially by the following categories:

❒ Adding Remote Gateways

❒ Configuring ANG IP Address

❒ Configuring Tunnel Protocols

❒ Configuring Virtual Subnets

❒ Configuring Routing Protocols

❒ Configuring Routing Interfaces

❒ Configuring Remote Connections

❒ Loading the Floppy Disk

Refer to Chapter 3 in the *RiverMaster Administrator’s Guide* for more detailed information about the concepts underlying ANG configuration.

Adding Remote Gateways

This section describes how to add a Remote ANG including its Name, IP Address, User Name and Password and tunnel Protocol.

To add a Remote ANG, perform the following steps:

1 Open the Configuration pullout.

2 In the list of Aurorean devices, expand the tree list under Systems (click the + symbol) and again under Remote Gateways as shown in Figure 120.

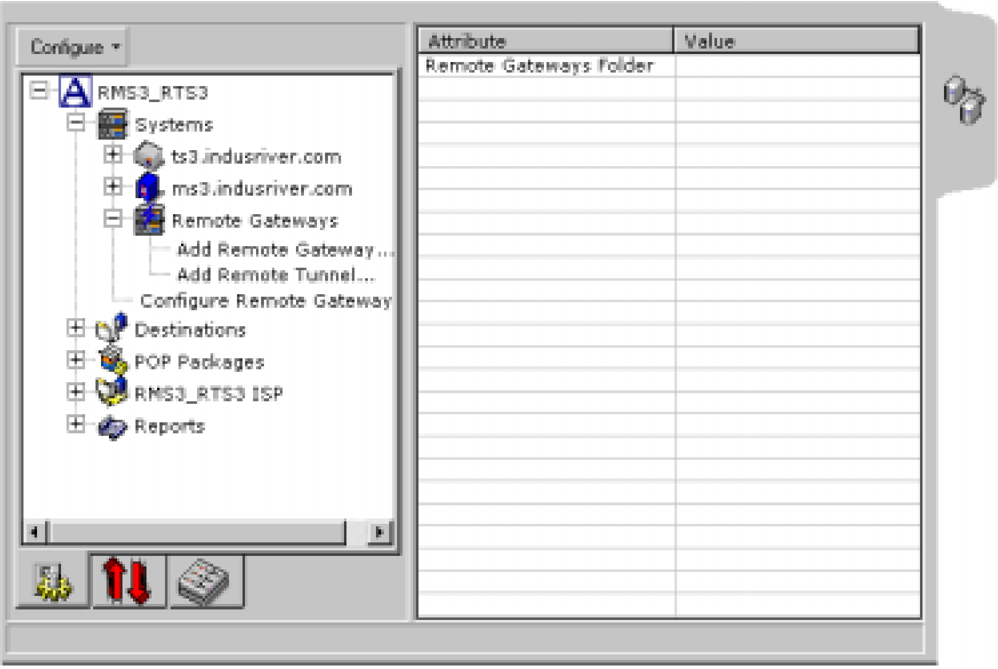
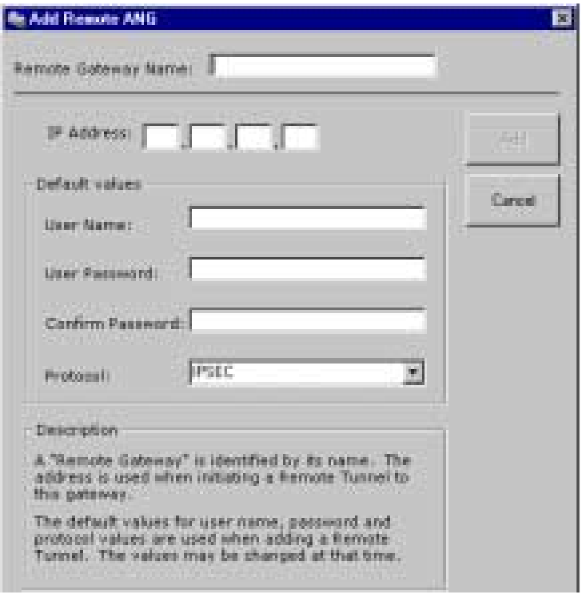


Figure 120 Add Remote Gateway

3 Click Add Remote Gateway.

The Add Remote ANG window appears as shown in Figure 121.



Protocol: IPSEC

A "Remote Gateway" is identified by its name. The address is used when initiating a Remote Tunnel to this gateway.

The default values for user name, password and protocol values are used when adding a Remote Tunnel. The values may be changed at that time.

Figure 121 Add Remote ANG Window

NOTE

Unless you are configuring a tunnel *from* the ANG / APS pair to a Remote ANG, you only need to enter the Remote Gateway Name and IP Address.

4 Enter a Remote Gateway Name and IP address in the fields provided.

5 Type a User Name, User Password and confirm the password.

This User Name and Password must also be registered in the authentication database in the ANG at the remote site by adding the user to a group (Refer to Chapter 6 for more information).

6 Choose the tunneling protocol: IPSec or PPTP.

7 Click Add.

The Remote ANG is added to the configuration on your local ANG. A message displays stating the Remote ANG was successfully added. Because the preceding configuration information is not immediately written to a floppy disk, we *strongly recommend* you repeat this procedure for all Remote ANGs you plan to add.

Configuring ANG IP Addresses

This section describes how to configure the ANG's name and Domain names, IP addresses and subnets, and Intelligent Client Routing. This action marks the actual start of the process to write information to the floppy disk.

NOTE

If the Remote Gateway configuration procedure is canceled at any point, it must be restarted here.

To set IP Address values, begin floppy disk configuration with these steps:

1 Under Remote Gateways, click Configure Remote Gateway.

The Remote ANG Configuration screen appears as shown in Figure 122.

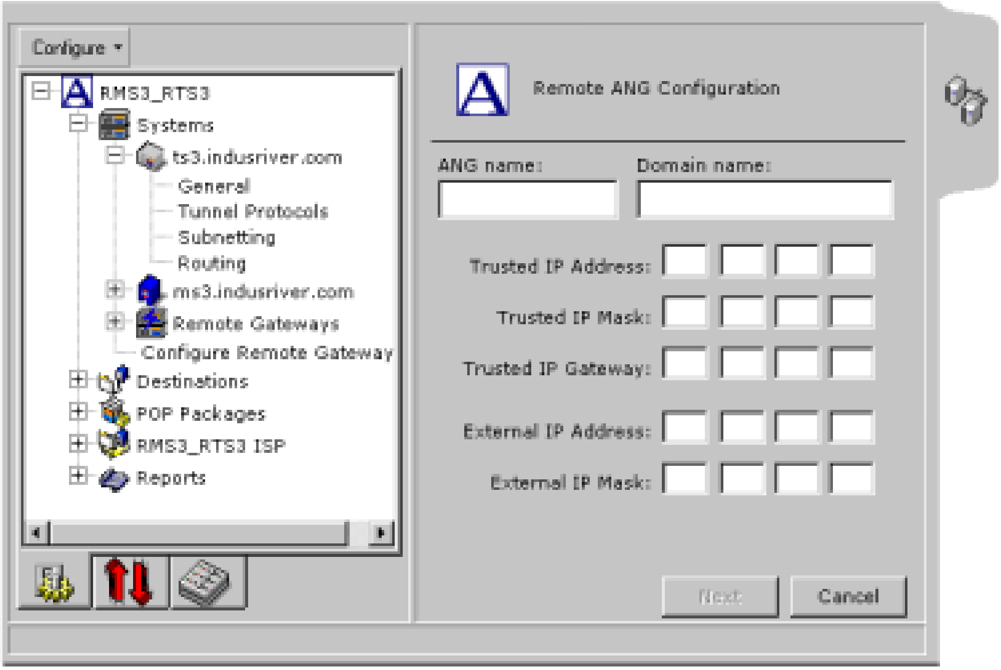


Figure 122 Remote ANG Configuration Window

2 Enter values in the open fields as follows:

- **ANG name**: A designation for the gateway
- **Domain name**: A Fully Qualified Domain Name (FQDN). Verify that the name is "fully-qualified" (not already in use within your domain) before entering it in this field. Domain names should follow the standard practice of period separators (for example, *APS7000.mycompany.com*)
- **Trusted IP Address** and **Subnet Mask**: IP addresses and subnet of the ANG's trusted interface
- **Trusted IP Gateway**: IP address of a gateway server on the trusted side of the network to which the ANG can route traffic
- **External IP Address** and **Subnet Mask**: IP address and subnet mask of the ANG's external interface

3 Click Next.

The Tunnel Protocols window appears with the General tab selected as shown in Figure 123.

Configuring Tunnel Protocols

This section describes how to configure the ANG's two supported tunnel protocols:

- ❒ Point-to-Point Tunneling Protocol (PPTP) developed by Microsoft, 3Com and others that uses Point-to-Point (PPP) protocol and Generic Routing Encapsulation (GRE) to route packets through the Internet.
- ❒ IP Security (IPSec) protocol developed by the Internet Engineering Task Force (IETF) that adds security extensions for encryption and message authentication to IP protocol.

For each tunnel protocol, you can configure authentication, encryption, and compression parameters. To set tunnel protocol parameters, continue floppy disk configuration with the following steps.

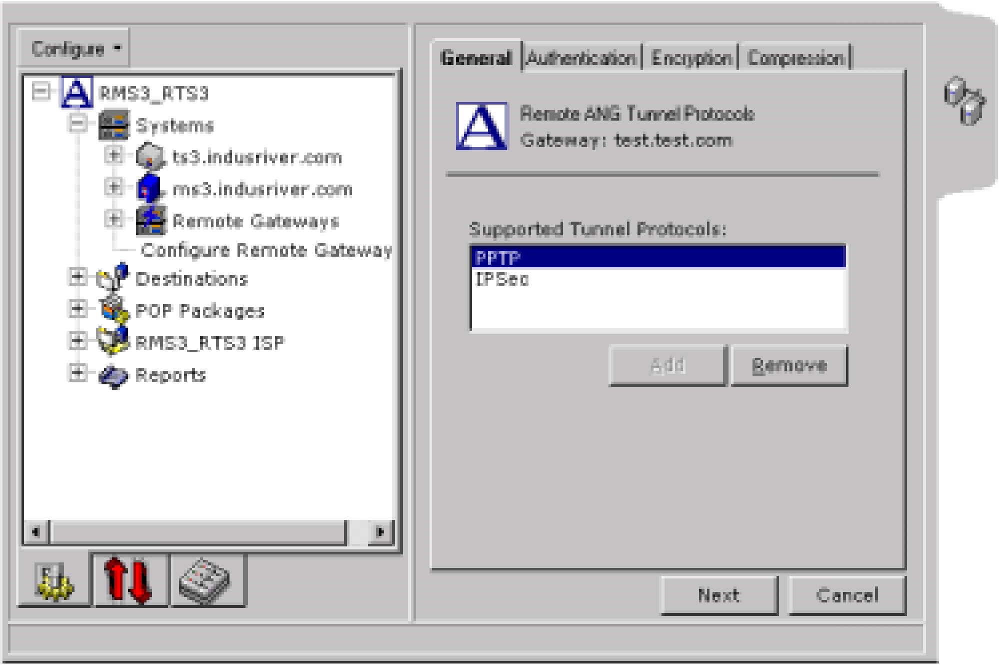


Figure 123 General Tab of Tunnel Protocols Window

1. If you want to prevent the Remote Gateway from using one of the tunnel protocols, select the protocol and click Remove.

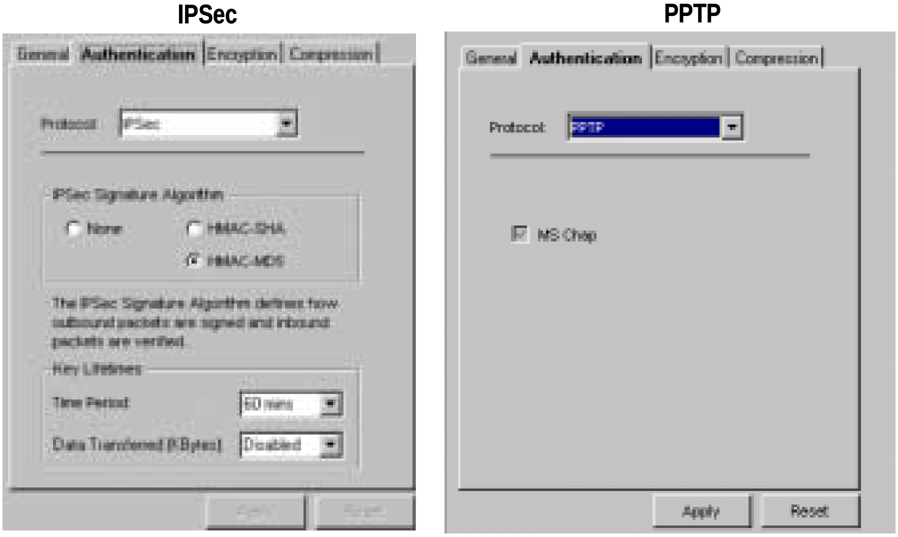
   By default, PPTP and IPSec are both enabled. You normally control protocol usage on a per group basis by selecting the protocol when you assign group policies (refer to Chapter 6 of the *RiverMaster Administrator's Guide* for instructions). If you want to globally disable a protocol, you can remove it from this list. If you have removed a protocol and want to reinstall it, click Add once and when the highlighted tunnel protocol pops up, click Add again. You are not required to click Apply.

2 Click on the Authentication tab.

Figure 124 shows the authentication parameters available for each tunnel protocol.

3 Do one of the following:

- Choose IPSec from the Protocol pull down menu.
  - Use the information in Table 18 to select the IPSec Signature Algorithm that determines how IPSec packets exchanged between the ANG and Aurorean users are signed and verified.
  - Use Table 18 to select the Time Period and Data Transferred values which set how long the key lifetime should last in terms of time elapsed or kilobytes amassed.
  - Click Apply.
- For PPTP, no additional work is required. Unlike IPSec, PPTP does not authenticate individual packets; instead, PPTP relies on user authentication using MS-CHAP. After the remote user is authenticated, all PPTP packets are allowed access.



IPSec

Protocol: IPSec

IPSec Signature Algorithm

○ None ○ HMAC-SHA ● HMAC-MD5

The IPSec Signature Algorithm defines how outbound packets are signed and inbound packets are verified.

Key Lifetimes

Time Period: 60 mins

Data Transferred (KBytes): Disabled

PPTP

Protocol: PPTP

☑ MS Chap

Figure 124 Tunnel Protocol Authentication Window

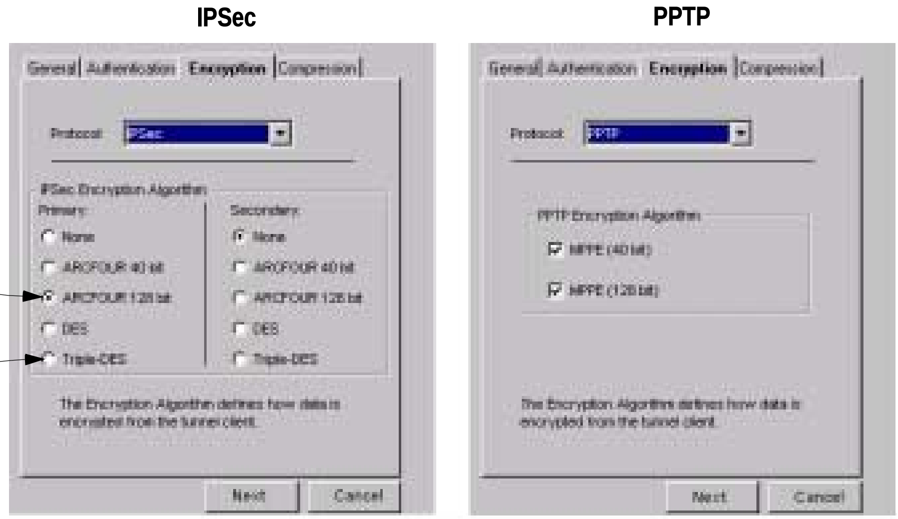
Table 18 IPsec Authentication Parameters

Parameter	**Explanation**
None	Disables the Signature Algorithm for IPSec packets; individual packets are no longer signed and verified during transmission.
HMAC-SHA	Enables hashing message authentication codes (HMAC) that are generated using the SHA cryptographic hashing function. HMAC-SHA is generally regarded as stronger, more secure cryptographic function than HMAC-MD5.
HMAC-MD5	Enables hashing message authentication codes (HMAC) that are generated using the Rivest MD5 message digest algorithm hashing function. While not as strong cryptographically as HMAC-SHA, HMAC-MD5 provides better performance.
Time Period	Interval after which a new key is generated. Default value: 60 minutes.
Data Transferred	Lifetime volume (in kilobytes) of the key after which a new key is generated. Default value: Disabled.

4 Click the Encryption tab.

5 Do one of the following:

- To set IPSec encryption parameters, choose **IPSec** from the Protocol menu. IPSec encryption parameters are shown in Figure 125. Select the IPSec Encryption Algorithm that determines how IPSec packets exchanged between Aurorean Network Gateways are encrypted.
- To set PPTP encryption parameters, choose **PPTP** from the Protocol menu. PPTP encryption parameters are shown in Figure 125. Select the Microsoft Point-to-Point Encryption (MPPE) algorithm that determines how PPTP packets exchanged between ANGs are encrypted.



IPSec

Protocol: IPSec

IPSec Encryption Algorithm

Primary:
○ None
○ ARCFOUR 40 bit
● ARCFOUR 128 bit
○ DES
○ Triple-DES

Secondary:
● None
○ ARCFOUR 40 bit
○ ARCFOUR 128 bit
○ DES
○ Triple-DES

The Encryption Algorithm defines how data is encrypted from the tunnel client.

PPTP

Protocol: PPTP

PPTP Encryption Algorithm
☑ MPPE (40 bit)
☑ MPPE (128 bit)

The Encryption Algorithm defines how data is encrypted from the tunnel client.

ARCFOUR is a public domain algorithm designed to work with RC4

DES is a government standard block cipher that uses a 56-bit key. Triple-DES uses three keys to achieve the equivalent of 112-bit encryption.

Figure 125 Tunnel Protocol Encryption Settings

Table 19 Encryption Parameters

Tunnel Protocol	Parameter	Explanation
IPSec	None	Disables encryption on the tunnel; because this results in a less secure connection, this setting is not recommended.
	ARCFOUR 40 bit	Enables a 40-bit key public domain algorithm that is designed to work with Rivest Cipher 4 (RC4), a stream-based cipher method that supports both 40-bit and 128-bit keys. Using RC4, data packets can be encrypted as they are received instead of in blocks.
	ARCFOUR 128 bit	Enables a 128-bit key version of ARCFOUR (described above).
	DES	Enables Data Encryption Standard (DES), a block cipher method that uses 56-bit keys. Using DES, data is encrypted in fixed-size blocks and packets are padded to become a multiple of the block size.
	Triple-DES	Enables a version of DES (described above) that employs a DES encryption with one key, a decryption with a second key, and then another encryption with a third key. The result is equivalent to DES with a 112-bit key.
PPTP	MPPE (40 bit)	Enables 40-bit key Microsoft Point-to-Point Encryption (MPPE) which generates a key based on a hash of the user’s password and invokes RC4 encryption.
	MPPE (128 bit)	Enables 128-bit key MPPE on the tunnel. .

6 Click the Compression tab.

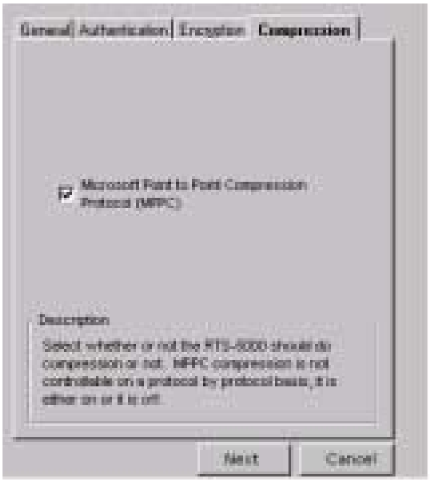
The Compression properties screen appears as shown in Figure 126.

7 Enable or disable MPPC as required.

For both IPSec and PPTP protocols, Microsoft Point-to-Point Compression (MPPC) is currently the only compression technique which you can select via this utility on the ANG (Stac LZS is available using the Command Line Interface). By default MPPC compression is enabled for both protocols.

NOTE

Compression settings are applied automatically to both tunnel protocols. That is, disabling compression on IPSec also disables compression on PPTP.



☑ Microsoft Point to Point Compression Protocol (MPPC)

Description

Select whether or not the RTS-8000 should do compression or not. MPPC compression is not controllable on a protocol by protocol basis, it is either on or it is off.

Figure 126 Tunnel Protocol Compression Settings

8 Click Next to save your changes. The Subnet Configuration window appears as shown in Figure 127.

To return the parameters to their original settings without saving your changes, click Cancel.

Configuring Virtual Subnets

This optional section describes how to create virtual subnets that serve as IP address pools for allocation to remote clients when they connect.

NOTE

Virtual subnets are configured for *terminating* ANGs only. If you are configuring an *initiating* ANG, skip to "Configuring Routing Protocols" on page 230.

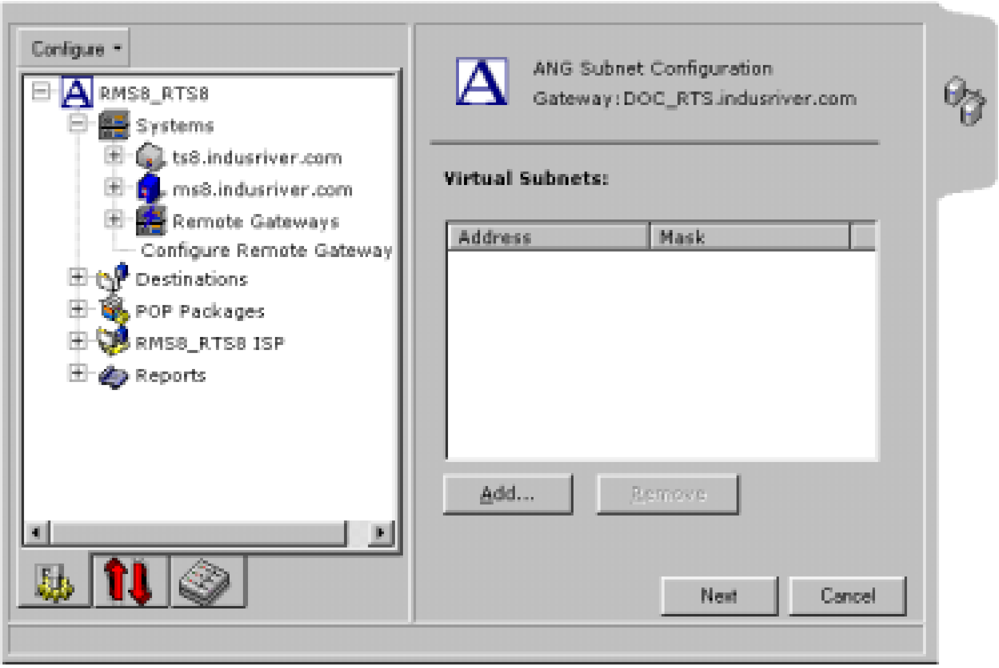
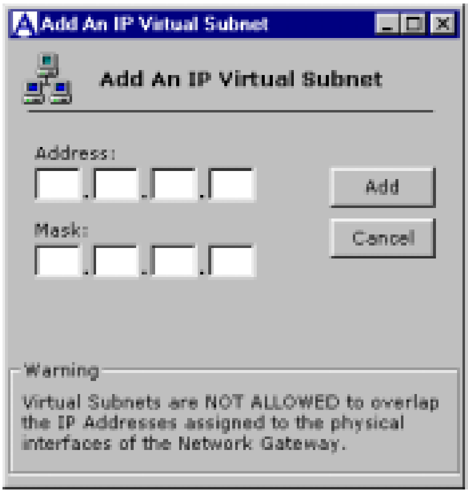


Figure 127 Subnet Configuration Window

To set up virtual subnets of IP addresses to allocate to remote users, continue floppy disk configuration with the following steps.

1 Click Add.

The Add an IP Virtual Subnet popup window appears as shown in Figure 128.



Virtual Subnets are NOT ALLOWED to overlap the IP Addresses assigned to the physical interfaces of the Network Gateway.

Figure 128 Add an IP Virtual Subnet Popup Window

2 Enter the starting address of the subnet in the Address fields.

You can use actual IP addresses from your network or non-routable IP address ranges (such as 192.168.x.x for a Class C network).

3 Enter a subnet mask to define the subnet range in the Mask field.

4 Do one of the following:

- Click Add to add the new virtual subnet.
- Click Cancel to close the window without saving your changes.

5 Repeat previous steps for each virtual subnet you require.

6 Click Add to save your changes and Next to bring up the Routing Configuration window as shown in Figure 129.

To return the parameters to their original settings without saving your changes, click Reset.

Configuring Routing Protocols

Configuring the routing behavior of the Aurorean Network Gateway consists of two general steps:

- ❒ Setting parameters for the two routing protocols supported, RIP and OSPF.
- ❒ Selecting routing protocols for each Aurorean Network Gateway Ethernet interface.

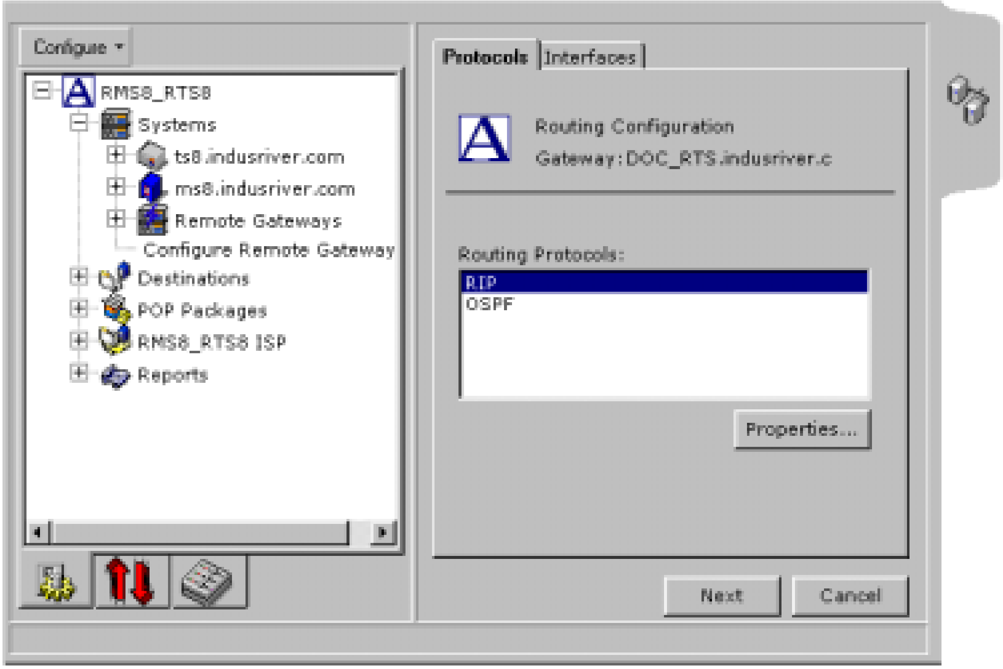


Figure 129 Protocols Tab of Routing Configuration Window

To access RIP and OSPF parameters for the Aurorean Network Gateway, continue floppy disk configuration with the following steps.

1 Do one of the following:

- To set RIP parameters, choose RIP from the Routing Protocols menu and click Properties; continue with Step 2. The RIP Configuration popup window appears as shown in Figure 130.
- To set OSPF parameters, choose OSPF from the Routing Protocols menu and click Properties; skip to "OSPF Properties" on page 232.

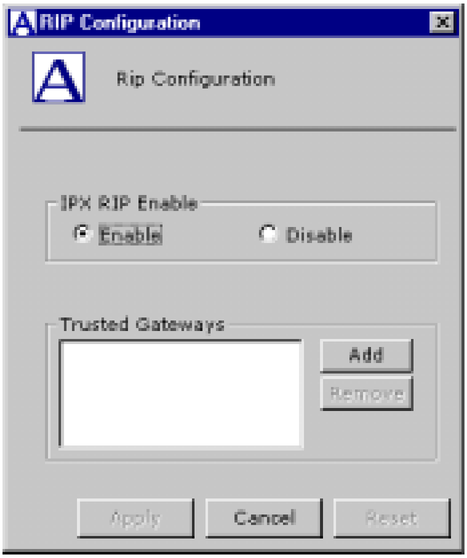


Figure 130 RIP Configuration Popup Window

2 In the RIP Configuration popup window, if you want to turn on RIP for IPX packets, click Enable under IPX RIP Enable; otherwise, continue with the next step.

3 Do one of the following:

- To allow the Aurorean Network Gateway to accept RIP updates from all routers on the same subnet, no further work is required. Skip to “OSPF Properties”.
- To configure “trusted” individual routers to supply RIP updates to the Aurorean Network Gateway, click Add and continue with the next step.

The Add A Trusted Gateway window appears as shown in Figure 131.

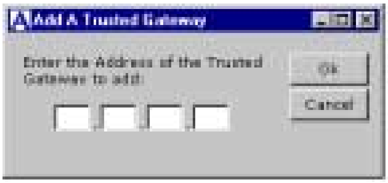


Figure 131 Adding A Trusted Gateway for RIP

4 In the Address field, type the address for the router that the Aurorean Network Gateway will accept updates from and click Add.

You can later modify this address or delete it using the Modify and Remove buttons.

5 Repeat Step 3 and Step 4 for each gateway required.

6 Do one of the following:

- Click Apply to save your changes and Cancel to close the window. If you want to configure OSPF on the ANG, continue with the next section, otherwise skip to “Configuring Routing Interfaces.”
- Click Cancel to close the window without saving your changes.
- Click Reset to return the RIP parameters to their default settings.

OSPF Properties

To enable OSPF on an interface, continue floppy disk configuration with the following steps:

1 With the OSPF Configuration window displayed as shown in Figure 132, type the area ID shared by the Aurorean Network Gateway and routers within the subnet in the OSPF Area ID fields.

.

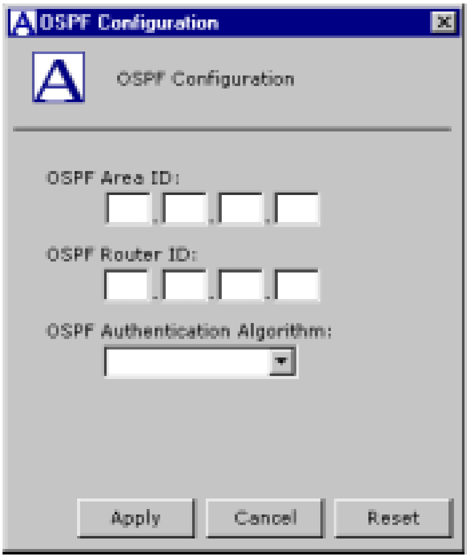


Figure 132 OSPF Routing Protocol Configuration

2 Type the IP address for the Trusted interface in the OSPF Router ID fields.

3 From the OSPF Authentication Algorithm menu, choose the authentication algorithm used by routers on your network.

If the routers on your network do not require passwords to accept OSPF updates, set the algorithm to None and continue with the next step.

4 Do one of the following:

- Click Apply to save your changes, click Cancel to close the window, and click Next to continue configuration. The Interfaces tab of the Routing Configuration window appears.
- Click Cancel to close the window without saving your changes.
- Click Reset to the return the OSPF properties to their default settings.

Configuring Routing Interfaces

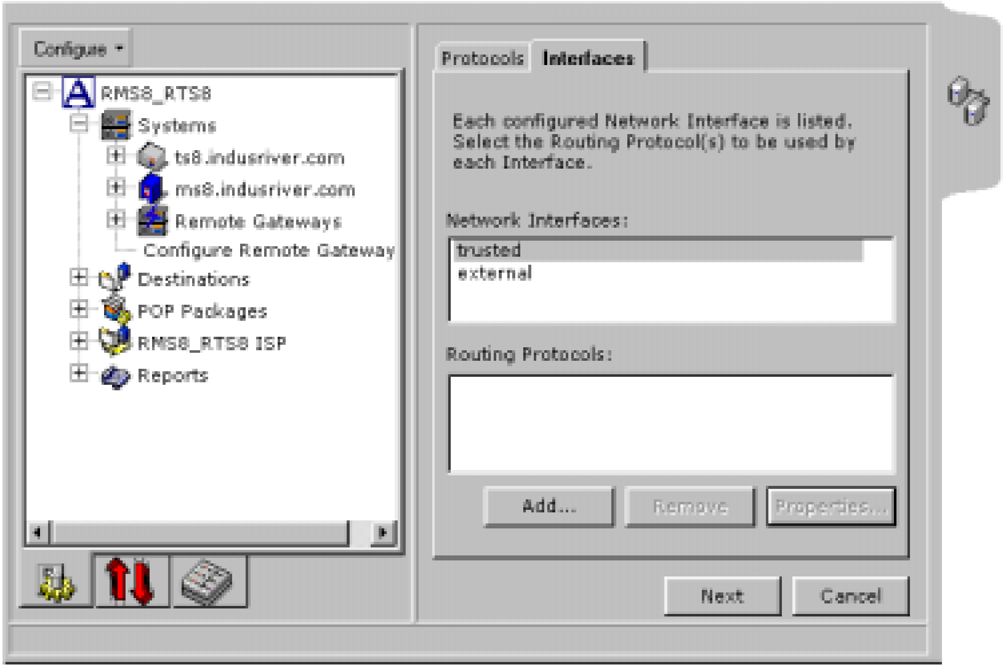
This section describes how to configure the ANG's two Ethernet interfaces:

- The *Trusted* interface should be connected to a protected network segment (one behind a firewall or router that offers protection against unauthorized access). Typically, you should enable a routing protocol (RIP, OSPF, or both) on the Trusted interface so that the Aurorean Network Gateway can advertise to other devices that its virtual subnets are reachable to the corporate network.
- The *External* interface can be connected to a network segment that resides outside a firewall and offers unfiltered access to the Internet. You must create a static route between the External interface and the router that serves as the gateway to the Internet. You cannot enable RIP or OSPF on this interface.

To add or remove a routing protocol from an interface, continue floppy disk configuration with the following steps:

1 Click the Interfaces tab in the Routing Configuration window.

The Interfaces tab in the Routing Configuration window appears as shown in Figure 133.



Each configured Network Interface is listed. Select the Routing Protocol(s) to be used by each Interface.

Network Interfaces:

trusted
external

Figure 133 Interfaces Tab in the Routing Configuration Window

2 Select the interface (Trusted or External) from the list under Network Interfaces.

The protocols already enabled for this interface appear in the Routing Protocols list.

3 Do one of the following:

- To add a protocol to the trusted interface, click Add and continue with the next step.
- To remove a protocol, select the protocol from the Routing Protocols list and click Remove. Skip to Step 5.

4 When the Add an Interface Routing Protocol window appears as shown in Figure 134, select a routing protocol and click Add.

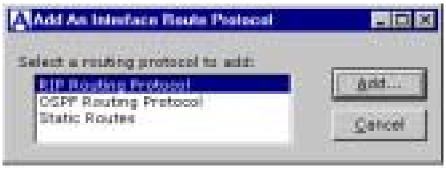


Figure 134 Adding a Routing Protocol

NOTE

For the External interface, you can only add or remove static routing. Because the External interface is optimized for tunnel protocols only, you cannot use RIP or OSPF on this interface.

5 Do one of the following:

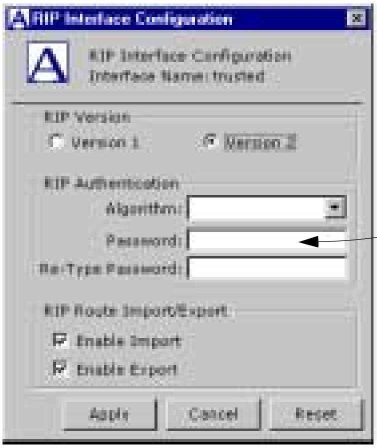
- If you are adding RIP to the interface, perform the steps in "Configuring RIP for the Interface" on page 236.
- If you are adding OSPF to the interface, perform the steps in "Configuring OSPF on an Interface" on page 238.
- If you are adding a static route to the interface, perform the steps in "Creating Static Routes" on page 239.

Configuring RIP for the Interface

To configure RIP on an interface, continue floppy disk configuration with the following steps:

1 In the RIP Interface window, shown in Figure 135, choose the version of RIP to use on this interface.

RIP Version 1 uses IP broadcast packets for periodic announcements of reachable subnets. RIP Version 2 is an enhanced version of RIP that uses IP multicast packets for announcements.



RIP Interface Configuration

RIP Interface Configuration
Interface Name: trusted

RIP Version
○ Version 1 ● Version 2

RIP Authentication
Algorithm:
Password:
Re-Type Password:

RIP Route Import/Export
☑ Enable Import
☑ Enable Export

These values are used to authenticate RIP updates from routers on the network

Figure 135 Routing Interfaces Configuration - RIP

2 In the RIP Authentication fields, choose the algorithm (simple or none) used by routers on your network.

If the routers on your network do not require passwords to accept RIP updates, set the algorithm to None and skip to Step 6.

NOTE

RIP update authentication is only supported by RIP Version 2. If the routers on your network only support RIP Version 1, you cannot enter values in the RIP Authentication fields.

3 Type the RIP authentication password used by routers on your network in the Password field.

RIP authentication passwords are used by routers to determine if they should accept updated routing information sent from another router. If your routers do not authenticate updates, leave this field blank and skip to Step 6.

4 Type the same password in the Re-Type Password field exactly as you entered it in Step 3.

5 Set the RIP Route Importing/Exporting options as follows:

- To allow the Aurorean Network Gateway interface to learn new routes, place a check next to Enable Import. If you enabled the Intelligent Client Routing feature, you should turn on Enable Import to allow the ANG to pass known reachable addresses to the remote client.
- To cause the ANG to advertise its known routes, place a check next to Enable Export. This setting is required to allow the ANG to advertise the reachability of virtual subnets to other devices on the network.

6 Do one of the following:

- Click Apply to save the RIP configuration changes, click Cancel to close the window, and click Next to continue configuration.
- Click Cancel to close the window without saving your changes.
- Click Reset to the return the interface’s protocol configuration to its original setting.

Configuring OSPF on an Interface

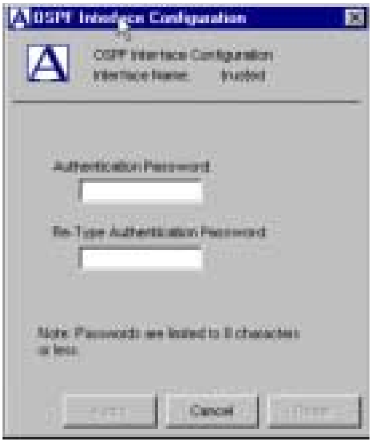
To enable OSPF on an interface, perform the following steps:

1 In the OSPF Interface window, shown in Figure 136, Type the OSPF password used by routers on your network in the Authentication Password field.

OSPF authentication passwords are used by routers to determine if they should accept updated routing information sent from another router. If your routers do not authenticate updates, leave this field blank.

NOTE

Passwords are limited to 8 characters or less.



OSPF Interface Configuration
Interface Name: trusted

Authentication Password

Re-Type Authentication Password

Note: Passwords are limited to 8 characters or less.

Figure 136 Routing Interfaces Configuration - OSPF

2 Type the same password in the Re-Type Authentication Password field exactly as you entered it in Step 2.

3 Do one of the following:

– Click Apply to save the OSPF parameter changes, click Cancel to close the window, and click Next to continue configuration.

– Click Cancel to close the window without saving your changes.

– Click Reset to the return the interface's protocol properties to their default settings.

Creating Static Routes

The trusted interface should be connected to a protected network segment - one behind a firewall or router that offers protection against unauthorized access. If you prefer to limit the routes the ANG learns or you do not use routing protocols on your network, set up a trusted Static Route.

CAUTION

The ANG **requires** that a static route be established to the Gateway router from the External interface to enable traffic to reach the Internet. The external interface may reside outside a firewall and offers unfiltered Internet access.

NOTE

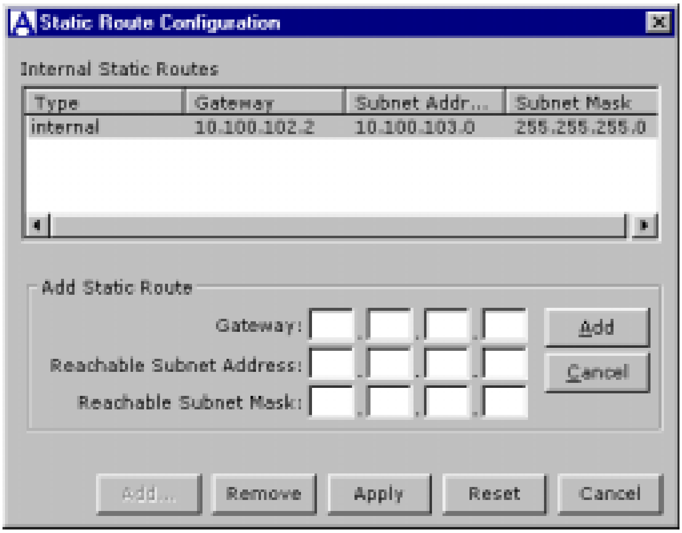
If you use static routes, the ANG will not broadcast IP pools. You must add a static route on your internal router for that subnet. The internal IP address of the ANG is the gateway.

To configure a static route between a Aurorean Network Gateway interface and another device, perform the following steps:

1. In the Routing Configuration window, with the Interfaces tab selected, choose the ANG Ethernet interface to configure (External or Trusted) and click Add.

2. In the Routing Protocol selection list of the Add an Interface Route Protocol popup window, double click Static Routes and click Add in the Static Route Configuration window.

   The Static parameter tab page is displayed as shown in Figure 137.



Type	Gateway	Subnet Addr...	Subnet Mask
internal	10.100.102.2	10.100.103.0	255.255.255.0

Figure 137 Static Routing Configuration Window

3 In the Gateway address fields, type the IP address of a gateway on this subnet.

For External interfaces, enter the IP address of the router that provides access to the Internet.

4 In the Reachable Subnet fields, type a starting IP address and subnet mask to define a subnet.

Packets received by the ANG are statically routed to the gateway you specified. To forward all packets to the gateway when there is no other reachable "next hop" address for a packet, enter an address of **0.0.0.0** and a subnet mask of **0.0.0.0**.

CAUTION

Configuring a default static route (0.0.0.0 / 0.0.0.0) on the *Trusted* interface of the ANG disables Intelligent Client Routing. Refer to "Intelligent Client Routing" in Chapter 3 for more information.

5 Click Add.

The static route you set appears in the Internal Static Routes display.

6 Do one of the following:

- Click Apply to create the static route, click Cancel to close the window, and click Next to continue configuration. The Remote Connections Configuration window appears.
- Click Reset to return the interface's protocol properties to their default settings.
- Click Cancel to close the window without saving your changes.

Creating Remote Connections

This section describes how to configure the connections between your ANGs. Connection and User names are employed to identify the ANGs at both ends of the tunnel connection. See Figure 138 for a graphical representation of an Aurorean Virtual Network meshed network.

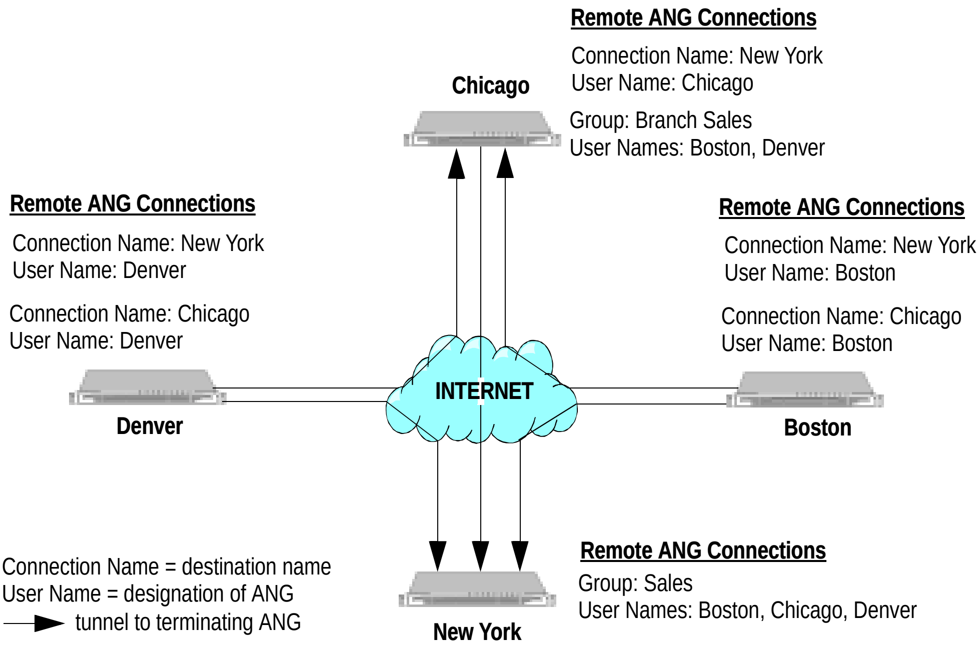
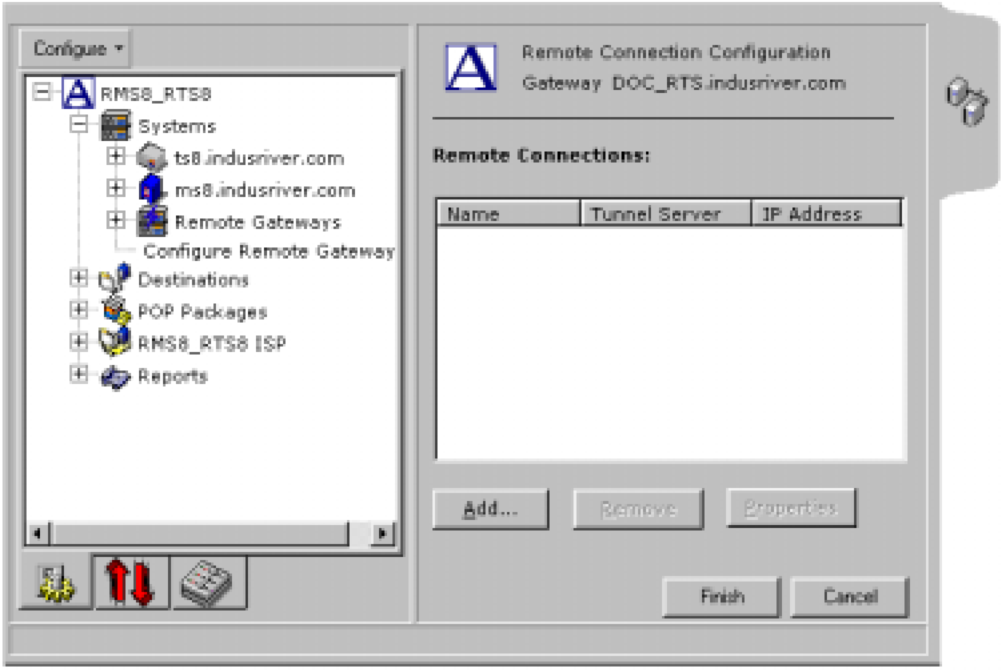


Figure 138 Aurorean Virtual Network Meshed Network Topology

To connect your configured ANG, continue floppy disk configuration with the following steps:

1. Click Add in the Remote Connection Configuration window, as shown in Figure 139.

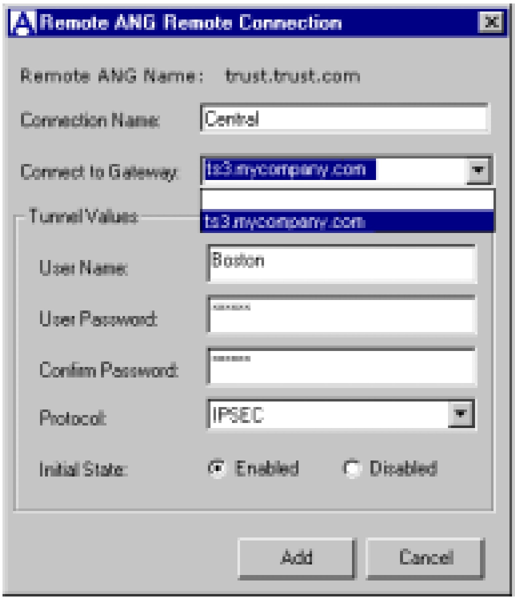
   The Remote Connection parameters window appears as shown in Figure 140.



Remote Connection Configuration
Gateway DOC_RTS.indusriver.com

Remote Connections:

Figure 139 Remote Connection Configuration Window



Remote ANG Remote Connection

Remote ANG Name: trust.trust.com

Connection Name: Central

Connect to Gateway: ts3.mycompany.com

Tunnel Values

User Name: Boston

User Password: ******

Confirm Password: ******

Protocol: IPSEC

Initial State: ● Enabled ○ Disabled

Figure 140 Remote Connection Parameters Window

2 Enter a name which describes the destination ANG of this ANG.

Choosing a Remote ANG name that matches the name of the *terminating* ANG of this tunnel connection will make it easier to view system activity and statistics later. Refer to Figure 138 for a graphical view of this configuration.

3 Choose an ANG from the drop down list in the Connection to Gateway field.

If you have configured other ANGs, they will appear in this list.

4 In the Tunnel Values section, enter a User Name.

Designating a User Name which matches the name of *this* ANG will make it easier to view system activity and statistics later. Only one user name is required for site-to-site users to access the connection.

NOTE

A User specified here also must be added to the connecting Local ANG User and Group database. Refer to Chapter 6, “Managing Users and Groups,” for instructions. Also be aware that you cannot use this floppy configuration utility to add Users and Groups to standalone ANGs which *terminate* tunnels. Only the Aurorean Policy Manager can perform this task. Refer to Chapter 3, “Configuring the ANG with Aurorean Policy Manager,” in the *Aurorean Installation & Service Guide* for instructions.

5 Enter a Password and Confirm Password for this user in the fields provided.

6 Select a tunnel Protocol (IPSec or PPTP) from the pull down list.

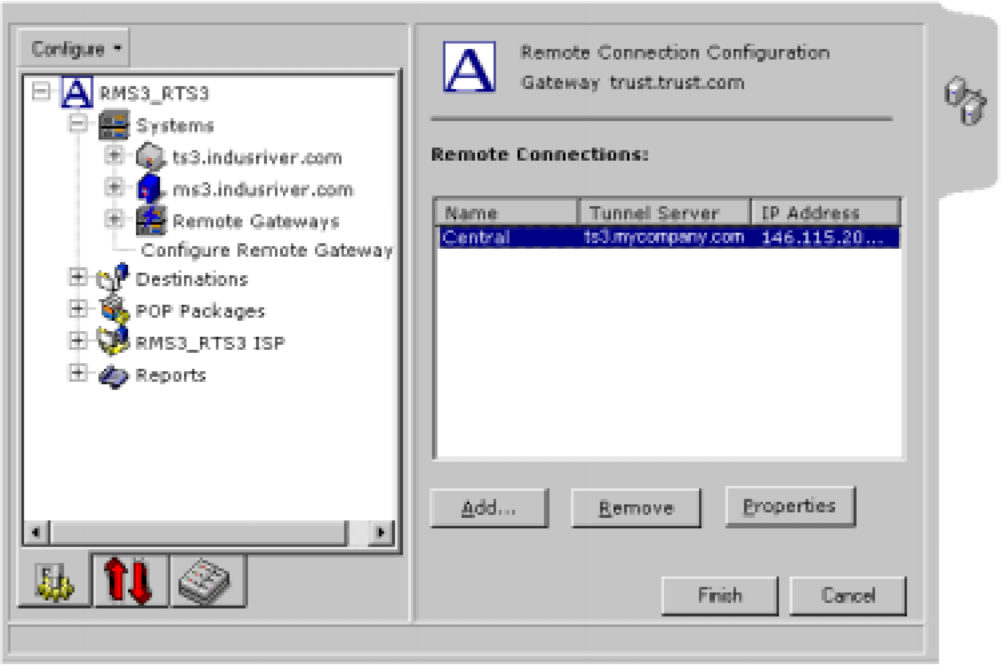
Between any two connecting ANGs in a fully meshed network, you can select different tunnel protocols.

7 Select the Initial State you want this ANG to default to upon startup.

If your Local ANG is up and running, the Remote ANG will be connected immediately with the default Initial State set to Enabled.

8 Click Add.

The new Remote ANG appears in the Remote Connection Configuration window as shown in Figure 141.



Remote Connection Configuration
Gateway trust.trust.com

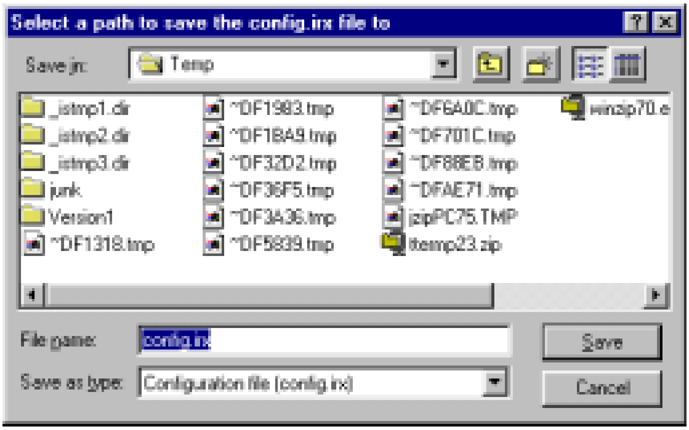
Remote Connections:

Name	Tunnel Server	IP Address
Central	ts3.mycompany.com	146.115.20...

Figure 141 Remote Connection Configuration Window

9 Do one of the following:

- Add another Remote Connection.
- Click Finish. The Save Configuration window appears as shown in Figure 142.



Select a path to save the config.irx file to

Save in: Temp

File name: config.irx

Save as type: Configuration file (config.irx)

Figure 142 Save Configuration Window

10 Select a directory, either on your computer, the A: drive, or another site on the network and click Save to store the configuration.

NOTE

When saving configuration information, you cannot change its default name `config.irx`. You may choose a different drive or directory but not a file name. Although you can enter a different file name and receive a message indicating RiverMaster successfully wrote the file, it will always be saved as `config.irx`.

This concludes floppy disk configuration on RiverMaster. Continue with the next section.

Loading the Floppy Disk

Configuring the ANG with the floppy disk at the remote location is simple. Perform the following:

1 Insert the floppy disk in the Floppy Disk drive.

2 Reboot the ANG.

3 Remove the floppy disk.

⚠ CAUTION

If you forget to remove the floppy disk, the next time the ANG is rebooted, any configuration changes you made with the APS will be replaced with the information stored on the disk.

The ANG is now up and the site-to-site connection running.

C

License Agreement & Support

This appendix describes the terms and conditions that govern the use of RiverMaster software (including the warranties), and provides contact information for obtaining technical support from Enterasys Networks.

Enterasys Networks License Agreement

PLEASE READ THIS DOCUMENT CAREFULLY BEFORE USING ENTERASYS SOFTWARE. BY USING THE SOFTWARE PRODUCT SHIPPED TO YOU BY ENTERASYS OR ITS DISTRIBUTOR ("LICENSED SOFTWARE") YOU ACCEPT THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE PRODUCT. YOU MAY RETURN THIS PRODUCT TO ENTERASYS FOR A FULL REFUND.

The Licensed Software is licensed, not sold, to you for use only under the terms of this license, which represents the complete agreement and understanding between you and Enterasys. Enterasys reserves any rights not expressly granted to you. You own the media on which the software is originally or subsequently recorded or fixed, but Enterasys retains ownership of all copies of the software itself.

License Grant

Enterasys Networks, 35 Industrial Way, Rochester, New Hampshire 03866 hereby grants to Licensee a personal, nonexclusive, non-transferable license to use the Licensed Software on the servers on which the Software is first installed ("Licensed Servers") and on an unlimited number of client processors, subject to the limit on simultaneous users as specified by the scope of the license that Licensee has purchased from Enterasys. Should one or more the above Licensed Servers be upgraded and / or replaced by other Enterasys servers purchased by Customer pursuant to Enterasys's then current upgrade policy, the license may be transferred and the Software may be used on the replacement server(s). This License shall commence upon the receipt by Licensee of the Licensed Software and shall continue until Licensee discontinues use or this Agreement is terminated. No ownership of the Licensed Software or any of its parts is transferred to Licensee.

Licensee may make copies of the Licensed Software in object code form for archival and backup purposes only. All copies (including copies of the documentation) must bear the copyright notice(s) and restricted rights legend contained in or on the original.

Except as expressly permitted by law without the possibility of contractual waiver, Licensee agrees that it will not attempt to reverse engineer, reverse compile or reverse assemble the Licensed Software or otherwise seek to gain access to source code for the Licensed Software.

Licensee shall take all reasonable steps to protect the Licensed Software and documentation from unauthorized copying and use. Licensee shall not, without the express written consent of Enterasys, provide, disclose, transfer or otherwise make available any Licensed Software, or copies thereof, to any third party.

Warranty

Enterasys warrants to Licensee that the Licensed Software will, when used in the specified operating environment, substantially perform in the manner described in its documentation, as it exists at the date of delivery, for a period of one year from the date of original delivery to the Licensee. Enterasys' sole obligation under this warranty shall be limited to using reasonable efforts to correct reproducible defects and distribute such corrections as part of the next scheduled maintenance release of the Software. Enterasys does not warrant that: (i) operation of any of the Licensed Software will be uninterrupted or error free, or (ii) functions contained in the Licensed Software shall operate in the combination which may be selected for use by Licensee or meet Licensee's requirements. Enterasys' warranty obligations shall be void if the Licensed Software is modified without the written consent of Enterasys.

EXCEPT AS SPECIFICALLY PROVIDED HEREIN, THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR ANY IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE.

Infringement Indemnification

Enterasys shall indemnify, defend and hold Customer harmless from and against any claims, actions, or demands alleging that the Licensed Software directly infringes any United States patent, trademark, or copyright, or misappropriates any trade secret right of any third party, provided that Customer promptly notifies Enterasys of any such claim, allows Enterasys to control the defense and provides reasonable information and assistance to Enterasys (at Enterasys' expense) in the defense of the claim. Customer shall permit Enterasys to replace or modify any affected Licensed Software to avoid infringement, or to procure for Customer the right to continue to use such Licensed Software. If neither of such alternatives is reasonably possible, Enterasys may require Customer to return the affected Licensed Software to Enterasys and Enterasys' sole liability in regard to such return shall be to refund the purchase price paid by Customer. Enterasys shall have no obligation with respect to claims, actions, or demands to the extent that they are based upon (i) the combination of Licensed Software with any items not supplied by Enterasys, (ii) any modification or change to the Licensed Software by Customer, or, (iii) any failure by Customer to implement modifications or replacements distributed by Enterasys that address any alleged infringement. This Section states the entire liability of Enterasys with respect to indemnification or liability for infringement or misappropriation of patents, copyrights, trademarks, trade secrets or other proprietary rights by Enterasys or the Licensed Software or any part thereof or by their use or operation.

Limitation of Liability

ENTERASYS AND ITS LICENSORS' TOTAL LIABILITY FOR ANY CAUSE OF ACTION ARISING IN CONNECTION WITH THIS AGREEMENT, AND REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR IN TORT INCLUDING NEGLIGENCE, SHALL BE LIMITED TO THE ACTUAL DOLLAR AMOUNT ENTERASYS RECEIVED HEREUNDER

FROM CUSTOMER FOR THE PARTICULAR PRODUCTS WHICH ARE THE SUBJECT MATTER OF THE CAUSE OF ACTION. IN NO EVENT SHALL ENTERASYS BE LIABLE FOR ANY LOST OR ANTICIPATED PROFITS OR SAVINGS, OR ANY INCIDENTAL, EXEMPLARY, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR IN TORT INCLUDING NEGLIGENCE, AND WHETHER OR NOT ENTERASYS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT PERMIT DISCLAIMERS OF IMPLIED WARRANTIES OR OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE DISCLAIMERS MAY NOT APPLY TO YOU.

Termination

Enterasys may terminate this license agreement and Licensee's right to use the Licensed Software if Licensee materially breaches the terms of this Agreement or fails to pay the licensee fee when due, and fails to cure such breach within thirty days of notice thereof by Enterasys.

International Provisions

Licensee agrees that it shall not directly or indirectly export the Licensed Software, individually or as part of a system, without first obtaining a license from the U.S. Department of Commerce or any other appropriate agency of the U.S. Government, as required. Diversion of products contrary to U.S. law is prohibited.

Applicable Law

The parties agree that this license shall be governed by the substantive laws of the State of New Hampshire and the United States. The exclusive jurisdiction for any dispute regarding this Agreement shall be in the United States of America or, for Licensees located in Europe, London, England. The parties expressly disclaim the applicability of the U.N. Convention on the Sales of Goods.

U. S. Government - Commercial Computer Software

This Licensed Software is Commercial Computer Software as provided in 48 CFR 2.101 and is licensed to U.S. Government agencies and personnel only with the rights set forth in this license. The use of the Licensed Software by the Government constitutes acknowledgment of Enterasys' proprietary rights in the Licensed Software. The manufacturer is Enterasys Networks, 35 Industrial Way, Rochester, New Hampshire 03866. The licensee or user of this product agrees not to remove any of the RESTRICTED RIGHTS legends and markings included in this software and associated documentation.

Technical Support

Enterasys Networks provides easy access to technical support information through a variety of services.

Support from Authorized Resellers

If you purchased your Aurorean Virtual Network server or software from an authorized Enterasys Networks reseller, contact the reseller for technical assistance. Most authorized resellers are qualified to provide a variety of services, including network planning, installation, maintenance, training, and customer support. If you unable to contact your reseller, contact Enterasys Networks directly as described below.

Support from Enterasys Networks

Enterasys Networks offers two ways of contacting customer support personnel.

On-line Services

To receive answers to technical questions on Aurorean Virtual Network products, send E-mail to:

support@enterasys.com

Please include your name, title, company, and phone number in all correspondence.

Phone Support

Enterasys Networks customer support personnel are available by calling **1 800-872-8440**. When you call, please call from a position where you can operate the RiverMaster management application or view the server's LEDs, and make sure you have the following information ready:

- ❐ State of the LEDs on both the front and rear panels of the server(s)
- ❐ A list of the error messages appearing in the RiverMaster message/alarm display
- ❐ Details about any recent configuration changes, if applicable

Enterasys Networks also recommends that you have this guide on hand when you call.

Index